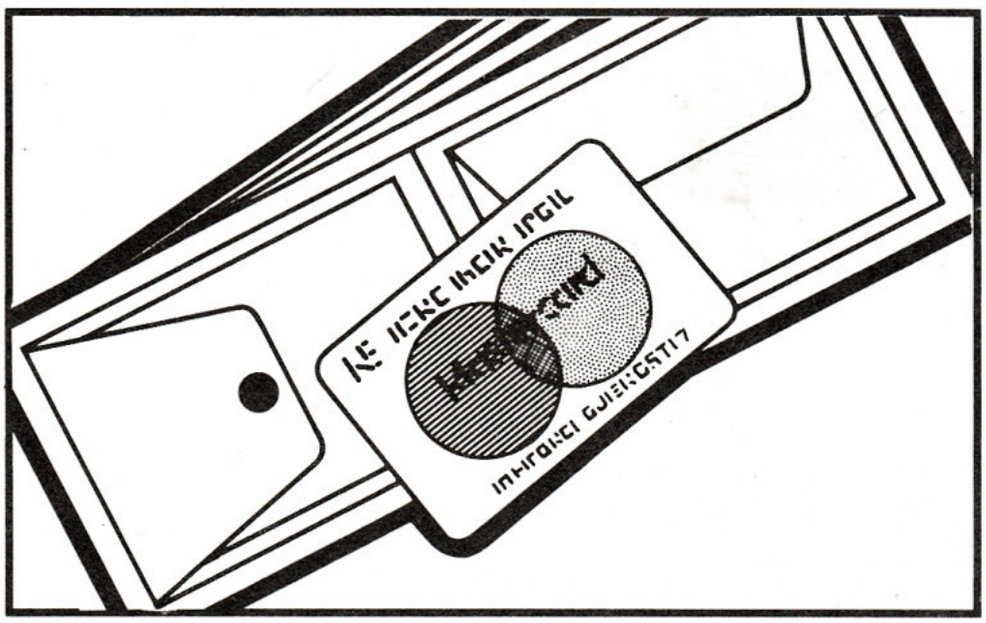
CREDIT CARD FRAUD

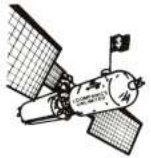


Burt Rapp

CREDIT CARD FRAUD

CREDIT CARD FRAUD

Burt Rapp



Loompanics Unlimited
Port Townsend, Washington

CREDIT CARD FRAUD
© 1991 by Burt Rapp
Printed in USA

All rights reserved. No part of this book may be reproduced or stored in any form whatsoever without the prior written consent of the publisher. Reviews may quote brief passages without the written consent of the publisher as long as proper credit is given.

Published by:
Loompanics Unlimited
PO Box 1197
Port Townsend, WA 98368

ISBN 1-55950-055-7
Library of Congress
Catalog Card Number 90-063591

This book is sold for informational purposes only. The publisher will not be held accountable for the use or misuse of the information contained in this book.

Contents

Introduction 1
Part I: Tasks 5
1. How Big Is The Problem? 7
2. Credit Cards: Uses And Abuses 11
3. Credit Card Security 21
4. Credit Card Forgery 29
5. Credit Card Frauds 41
6. Consumer Victimization 61
Part II: Tactics 65
7. Police Response 67
8. Prevention 71
9. Counter-Attack: Striking Back At Fraud 85
Part III: Tools 97
10. Tools For The Job 99
11. Information Management 101
Glossary 121
Index 125

Introduction

There's one main reason why credit card fraud is widespread and remunerative: credit cards are big business today. According to the 1990 *World Almanac,* there were a total of 201 million Mastercard and VISA accounts in 1988. The average monthly balance was $1,200, according to figures from the American Bankers' Association. The average credit card transaction was $63 in 1988, up from $60 in 1987.

Money Magazine, based on its 6th national survey of its readers, concluded that 80% of Americans have credit cards. Sixty-four percent have only retail store credit cards, while 61% have bank credit cards. These figures overlap, because many people have more than one card. The net result, according to the Federal Trade Commission, is that credit card fraud amounts to about $500 million per year.

One effect of credit card proliferation has been to increase opportunities for theft. Before credit cards, it was necessary to rob the victim, or pick his pocket, to steal his money. Stealing his property usually required burglarizing his premises. Today, simple credit card fraud schemes allow low-risk theft, without the perpetrator ever needing to come into contact with his victims. Modern technology, in the form of television shopping clubs and other "telemarketing" schemes, help the thief as much as the legitimate customer.

Both police officers and private citizens need to have a working knowledge of how credit card frauds operate. Of the two, private citizens need it more, because they're the victims, whether they're merchants victimized by fake credit card passers, or just "Joe Sixpack," who finds unfamiliar charges debited to his account.

This book is for police officers and civilians alike. It's an investigation guide and practical manual for the police officer charged with a credit card fraud investigation and its follow-up. For the civilian, it provides a comprehensive working knowledge of how police investigators conduct credit card fraud follow-ups. One disappointing surprise to the citizen and taxpayer will be the extremely low priority police agencies and public prosecutors give to credit card scams.

Very importantly, this book provides a basis for appraising the chances of avoiding future frauds, and lays out steps to enhance the odds. This is valuable information for citizens, and provides a framework for community relations officers working with various crime prevention programs.

This is critically important, because with every step taken to increase security, fraud artists find ways to defeat them. As we'll see, high-tech means of making credit cards difficult to forge are not very effective when we consider the overall picture. It's very easy to obtain credit cards under fraudulent circumstances, or to steal them.

Although federal law mandates that a cardholder is liable for only the first $50 if he doesn't report a card's loss promptly, the effects of credit card fraud reach right back to him. In one racket, a fraud artist claims that he never received the merchandise, and this results in a charge-back to the merchant. This, in turn, results in higher prices to cover his losses. Some merchants, if their charge-backs exceed a certain percentage, can find themselves stripped of credit card privileges.

Those of you who have read other books in the Loompanics Criminal Justice Series may have noted that we approach the topics somewhat differently from other texts. We'll cover this topic in the following order:

Tasks

Tactics

Tools

The reason is that this is the logical way to do it. We need to know the extent of the problems facing us before we can decide on how to handle them. Consequently, we lay out the tasks. Once we know the tasks, we can discuss and select the tactics which are most effective. Knowing the tactics, we'll be able to select the tools for the job.

Tasks will cover the nature of the problem, including the definition and extent of the crime. We'll look at the perpetrators, their various types and categories, and how they work. We'll study their techniques and motives.

Tactics will cover the police and investigator's response to credit card fraud. This will include obtaining statements from victims and witnesses, gathering physical evidence, and follow-up procedures.

Tools will cover specific items of equipment and their use in the investigations. Some of these are fairly high-tech, and can be very costly. In fact, the large computer systems companies such as American Express and Diner's Club use are out of reach for most police departments and private security agencies. Nevertheless, it's possible to cope with the problem, because the number of credit card crimes committed by professionals is low compared to the number of cards in circulation.

This book is directed mainly at the many small police agencies in the United States, and the small to medium size security departments serving retailers. It's also for small retailers who are their own security departments. Large agencies have the manpower and technical re-

sources to cope with the flood of credit card and other frauds within their jurisdictions. Small agencies often don't even have a fraud detective, only a general-purpose investigator who is responsible for follow-up on all crimes. Small agencies have to make do with less, at a time when crime is spilling over into suburban and rural areas. This book will help.

Part I

Tasks

Just as there are many different kinds of credit cards, there are many varieties of credit card fraud. In this section, we'll first look at the scope of credit card fraud. Then we'll examine the kinds of cards available and how they are used. We'll continue with a close look at credit card security: what safeguards are built into cards and into the system through which they're used. Finally, we'll reveal every known method of credit card fraud: an amazing collection of criminal techniques for manipulating the credit card system.

1

How Big Is The Problem?

Credit card fraud does not exist in a vacuum. Often, credit card fraud ties in with other crimes, such as burglary, mail theft, pocket picking, and passing falsified checks.

This is a two-edged topic because credit card fraud works both against the bank or company, and against the consumer. The American Bankers Association recently polled 1,200 banks, and found that 25% of them reported cases of fraud by a customer. By contrast, 13% of them reported fraud against a customer.[1]

We have to be very careful in interpreting these figures. It would be naive to say that customers cheat banks more than banks cheat customers. It's important to remember who is doing the reporting.

We'll first discuss frauds against banks and issuers, because of the tremendous variety of techniques that enterprising fraud artists have devised. Another chapter will deal with frauds by banks and companies against their clients.

In 1984, there were already 577 million credit cards in circulation.[2] This amounts to two cards for every American. With so many credit cards in circulation, it's impossible to avoid misuse.

Nobody really knows how many credit card frauds occur in this country each year. The main reason is that

many companies don't bother to report them to the police. Indeed, as we shall see, many companies accept a percentage of their orders as fraudulent, as "part of the cost of doing business." One estimate was that $4 billion in fraud losses took place in 1984.[3] Presumably, the amount has increased proportionately since then.

The Bank Administration Institute reported that the average number of automatic teller machine frauds per financial institution in its survey was 62 in 1988. This is a drop from the average of 390 frauds reported in 1986, according to the institute.[4]

One explanation is increased security measures by banks. Another is decreased frequency of reporting. This is the problem that prevents the compiling of accurate statistics on credit card frauds. A bank or credit company needs to preserve its image, to retain the confidence of its customers. The image is one of Gibraltar-like security. In the thinking of top executives, anything that impairs this image is destructive. Some bank executives, like other businessmen, conclude that the cost of frauds is "part of the cost of doing business," and accept a certain percentage of fraudulent transactions.

If banks and credit card companies don't report frauds, where does this leave the police investigator? Actually, there are other ways of entry into the problem. Credit card crimes do not occur in a vacuum.

This is because obtaining credit cards fraudulently usually involves another crime, and because credit cards are often helpful in committing other crimes. An example is using a stolen credit card to rent a car, which the renter then proceeds to sell to a chop shop.

The investigator must be aware that a credit card fraud is often merely the tip of an iceberg, and must be prepared to follow the trail that can lead to a string of related offenses.

Sources

1. Associated Press, December 29, 1989.
2. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #5, May, 1984, p. 4.
3. *Ibid.*, p. 6.
4. Associated Press, December 29, 1989.

2

Credit Cards: Uses And Abuses

The story of the credit card in this country begins around the turn of the century, when several hotels began issuing them to selected customers. During the early part of this century's second decade, some department stores passed out embossed metal plates to their better customers. These were a start at automating credit cards, as it was necessary only to press a multi-part carbon form against the card, using a special press, to get an imprint of the client's name, address, and account number. The early 1920s saw the introduction of gasoline credit cards.[1] Almost everyone has seen credit cards, and has a notion of how people use them. However, few people are aware of the exact differences between various types of credit cards.

Credit Card Types

There are five categories of credit cards.

Travel and Entertainment Cards

These were among the earliest types of credit cards, restricted to people with incomes large enough to afford them, and to corporate card-holders. The first such credit card issuer, Diner's Club, began in New York in 1950. American Express got into the credit card business in

1958. A small number of banks also started their own credit cards.[2]

T&E cards are for the most part businessmen's charge cards, used to provide both convenience and permanent records for tax deductions. They also cater to the rich, who frequent merchants who accept these cards. American Express, Diner's Club, and Carte Blanche are the three major American T&E card companies.

These cards allow the bearer to travel with minimal cash in his wallet, and to pay for services by presenting the card and signing a credit card slip. Many restaurants, and retailers, as well as hotels, motels, car rental agencies, florists, and other businesses accept one or more of these cards. A business traveler can pay for airplane tickets with such a card, use them to cash checks, and even obtain cash. American Express will advance a card-holder cash at any office in many countries of the world.

There is a price to pay for these services. There's an annual fee for each card, whether the card-holder uses it or not. The American Express Green Card, for example, costs $55 per year. The Gold Card, with higher credit limits, costs $75 per year. American Express accounts must be paid in full every month. Other cards allow installment payments and charge interest on the outstanding balance.

Corporate credit cards, of course, are paid by the corporation which provides them for its executives. Indeed, one or more credit cards are often part of the perquisites, or fringe benefits, that a company executive enjoys. These allow him to charge purchases and services, up to a limit, at the corporation's expense. The presumption is that the executive will use his card for business expenses, but in reality, nobody cares, as long as he remains within the agreed limit. Expense account abuse is a normal way to avoid paying taxes on income.

A major difference between T&E cards and bank cards is that the limit is much higher. A corporate T&E card-

holder can accrue charges up to many tens of thousands of dollars, because the corporation is responsible for payment. His "limit" is that imposed by his superiors in the corporation.

An individual card-holder works within a limit imposed by the card issuer, which considers his income, payment history, and credit rating.

Bank Credit Cards

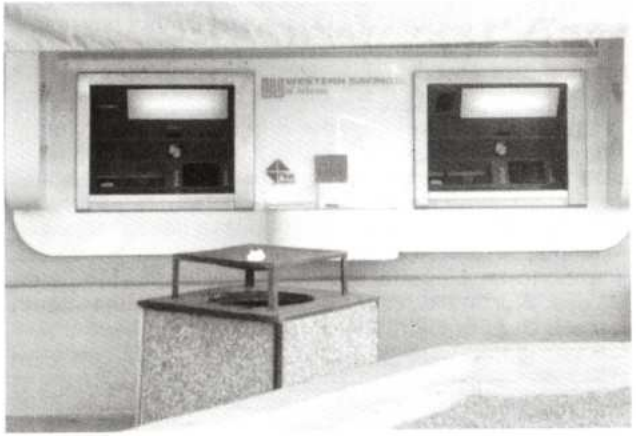


Figure 1

This pair of automatic teller machines outside a savings and loan association provides electronic banking 24 hours a day. This easy access isn't an unmixed blessing, however.

These are the most common, and are usually one of several types: ATM Cards, "Mastercard," and "VISA." The difference between them is that the Mastercard is a true charge or credit card, and the VISA card is a "debit" card. The ATM card is also a debit card, as it enables with-

drawals from a savings account at an automatic teller machine (see Figure 1), but does not allow charging of any outside purchases.

Bank credit cards began during the 1950s, but did not take off until the next decade, when loose associations of banks introduced area-wide and national bank cards. During the 1960s and 1970s, the two giants, Mastercard and VISA, emerged and came into their final forms.[3]

With a credit card, the bank bills the card-holder for charges at the end of each month. This is linked to a finance plan whereby if the card-holder cannot pay in full, he can pay the minimum payment and defer paying the balance until later, when he pays interest on the loan.

Finance charges vary from bank to bank, and from state to state. State banking law regulates the maximum interest rate in many states, the lowest being Connecticut's 15%, and the highest Wyoming's 36%. Many states do not impose a maximum interest rate, and rates vary according to "free market" conditions. These states are: Alabama, Arizona, California, Delaware, Georgia, Idaho, Illinois, Iowa, Montana, Nevada, New Hampshire, New Mexico, North Dakota, Oregon, South Carolina, South Dakota, Utah, and Virginia.

Some banks maintain low interest rates on bank card accounts. A list of banks charging less than 16.4% is available from:

Bankcard Holders of America
560 Herndon Parkway, Suite 120
Herndon, VA 22070

Most banks and savings & loan associations now impose a yearly charge for their Mastercards and VISA cards. This is in the $20 range for a Mastercard. The premium "Gold Card" fee is higher. The charge is $48 for Chase Bank's Gold Card, for example. A small number of banks still don't have an annual charge. A list of banks not charging annual fees is also available from Bankcard Holders of America.

A debit card is always linked to a savings or checking account, and the bank immediately deducts the amount from the account balance. The card-holder receives a statement at the end of the month listing the charges against his account, and the balance on the date of the statement. Some debit cards also have lines of credit, allowing the card-holder to charge up to a limit beyond his account balance, and paying interest on the borrowed amount.

Many debit card holders don't realize that their cards are a greater liability than credit cards. This is because use of an ATM card enables the fraud artist to raid the customer's entire account. As we'll see in the "Fraud" chapter, sometimes the cardholder is under duress.

As partial protection against this threat, banks impose a daily limit on cash withdrawals from ATMs. Typically, a debit card, such as VISA, has a limit of $200 or $300 per day. Other limits, to defeat fraud artists who charge purchases in a "blitz" pattern, are on daily credit limits and number of daily charges. Security Pacific Bank, for example, sets a credit card merchandise limit of $600, or 9 transactions, for one day. The two-day total may not exceed $900, or 12 transactions. The three day cumulative is $1,200, or 15 transactions, and the four day limit is $1,500, or 18 transactions.

Air Travel Cards

These are special-purpose cards issued by airline companies, used to charge air fares throughout the airline's network. One such is TWA's "Getaway Card," which TWA advertises an "an extra line of credit." The card-holder can charge his air fare on the card, and save his other credit cards for other expenses, according to their brochure. TWA also allows the user to charge fares on other airlines, on condition that he travel part-way on

TWA and book his passage through TWA or a travel agent. The card itself is free, but a finance charge applies if the card-holder doesn't pay his entire balance with each statement.

Oil Company Credit Cards

These are cards for cashless purchase of fuel and services at gas stations. Originally, they were issued by each oil company for use only at its own stations. These companies used to be eager to issue cards, because this created a captive customer, as oil companies did not honor each other's cards, and the card-holder was able to buy gas only at stations operated by the card issuer. A traveler or businessman had to have a sheaf of gas credit cards, one for each oil company chain, to allow him to buy fuel wherever he happened to be.

Gas stations changed over the years, and independent operators became reluctant to turn away business because the client had another company's credit card. Some began accepting other companies' cards, and once bank cards came into wide use, it was possible to charge service station purchases against many types of cards.

Retail Store Charge Card

These are issued by various retailers, such as clothing, department, and discount outlets. They bear the store name, and are good only in that store. There's usually no charge for this type of card, because it's a way of building up a captive clientele, as oil company cards were in their early days.

Credit Cards in Practice

There are two ways in which a card-holder uses a credit card; to obtain merchandise or services, and to obtain

cash. The exact mechanism varies with the type of card and the locale.

Cash

The card-holder slips his card into the slot of an automatic teller machine, punches in his PIN (personal identification number), and the amount of cash he wants. The machine spits out the money, a transaction receipt, and the card.

In some cases, the card-holder can get cash over-the-counter, such as at an American Express office. Some cards are check guarantee cards as well, allowing the bearer to cash a check up to a certain limit.

Merchandise

The credit card issuer is also the redeemer of charges to the cards, accepting charge slips from merchants and paying them the amount of the billing less a percentage for handling the transactions. They charge the merchant a fee based on a percentage of the monthly billing. This varies between 2% and 8%, in most cases, and is linked with the volume of billing.

Why does the bank or credit card company charge the merchant, instead of the merchant charging the bank for handling the extra paperwork? The reason is simply power politics, which in this case is the advantage the large company has over the small one. The small businessman needs the bank much more than the bank needs him. The credit card is a common way of paying for goods and services, and the merchant who refuses to accept them is simply left out in the cold. This is why the banks and credit card companies can dictate terms to the small merchants, and to many large ones, as well.

One of the few exceptions is the supermarket and grocery field. The profit margin is simply too small to ab-

sorb the extra amputation of several percent. Most supermarkets and groceries deal in cash or check only. Accepting checks does involve handling extra paperwork, but not paying a percentage to the bank.

For small purchases at merchants other than groceries, the card-holder presents his card to the clerk, who may check it against a "hot list" of stolen or invalid cards, and if it passes, the clerk puts it face up into a hand press which uses the card's embossed numbers to print a charge slip. The customer signs the charge slip, writes his telephone number if requested, and the clerk separates the charge slip copies and gives the carbon and second sheet to the customer.

Figure 2

This card reader is a "point of sale terminal," which electronically verifies the card's validity, and debits the card holder's account for the purchase. This model even prints out a transaction receipt, in duplicate, for the customer to sign.

Some retailers have electronic checking to verify the card's validity. The clerk slips the card into the slot of a card reader (see Figure 2), which is connected to a central computer. This verifies that the card is good, and that there's enough credit left in the account to pay for the purchase.

For larger purchases, it's necessary for the retailer to obtain authorization for each purchase over the "floor limit." This is the amount, above which the retailer is responsible if he accepts the card without authorization, and it later turns out to be invalid, or the account overdrawn.

There are several booby-traps for the merchant in these procedures. First, the authorization merely verifies that the card is valid, and that the card-holder has enough credit reserve to cover that particular purchase. It does not, except for a few systems, debit the card-holder's account immediately. In practice, the card passer can make the rounds, obtaining several authorizations, and charging a spate of high-dollar purchases before it all catches up to him.

The merchant who accepts telephone orders, without a customer signature on the charge slip, takes a risk if the customer disclaims the purchase, or claims that he never received delivery. This is especially true for purchases of only a few hundred dollars, delivered to out-of-state addresses. Even with a delivery receipt, collection or prosecution is very difficult. Collection agencies rarely want to touch these cases, because the expense involved in trying to collect makes it impractical.

Some services are extremely vulnerable, because they don't bill the credit card issuer immediately. Auto rental agencies, for example, are extremely interested in verifying the card before allowing a stranger to drive off in a late-model rental car. Once the card is verified, with a card reader connected to a central computer, the clerk makes

out a charge slip and holds it until the customer returns the car. At that time, the clerk adds up all charges and fills in the charge slip for collection. For this reason, charges don't appear in the card-holder's account until some time after he returns the car. This allows many car rentals on one card, far beyond the card-holder's ability to pay.

Sources

1. *Charge It!*, Terry Galanoy, New York, G. P. Putnam's Sons, 1980, pp. 60-61.
2. *Ibid.*, p. 62.
3. *Ibid.*, p. 68-72.

3

Credit Card Security

There are two basic approaches to security; the "lock every door" approach, and the "allowable loss" philosophy. It's critically important to understand this, because it explains the reasoning behind various security practices.

The "lock every door" approach is typical of public agencies, such as the police and fire departments. Theoretically, at least, they investigate every case, and fight every fire, regardless of cost. The most conspicuous example is prosecution of murder. The criminal justice system will spend millions of dollars to prosecute and execute a murderer, although the victim may have had his life insured for only ten thousand dollars, or perhaps nothing at all. We'll see, however, that the police do not pursue non-violent crimes with the same vigor.

The "allowable loss" approach considers cost-effectiveness in designing security measures, and is typical of private businesses. Security executives weigh every proposed security technique, calculating its cost against the amount of money it's supposed to save, before adopting any of them. Banks, retailers, and credit companies don't like to publicize it, but they're well prepared to accept a certain percentage of losses, calculating that they can pass the cost on to their customers.

Some of the nation's largest companies in catalog sales, for example, "have become resigned to accepting large

dollar amounts of credit card and check fraud loss as part of the cost of doing business."[1]

One company doing $200 million per year accepted a $500,000 loss with equanimity. Another, charged 2.4% by the bank as a credit card processing fee, accepted a 2.4% fraud loss rate.

No security system is perfect, especially not one that passes through millions of hands, as do credit cards. The best for which credit card security officers can hope is to make it difficult enough for fraud artists that they'll find it unproductive to try to carry out any frauds. What actually happens, though, is that a small number still try, and often succeed. The reason is that each new security measure suggests a new way to defeat it. As we shall see, there are some forms of credit card fraud and misuse impossible to prevent.

Security Measures

Security measures are becoming more rigorous. Cards are today much harder to forge than before, and new security procedures make it harder to misuse a lost or stolen card. It's actually easier to steal a genuine card. Let's trace the development of credit card security measures.

Signature Strip

The earliest method of ensuring security was to have the card-holder sign his card upon receipt, for comparison with the signature on the charge slip for each purchase. This was not very effective, for several reasons, but it continued until better means arrived.

Some people are skilled in signature forgery, and these gravitated naturally towards crimes involving such forgeries. Another problem is that people often sign their

names differently because of fatigue, illness, and other factors. Clerks are not experts in detecting forgery, or separating forged signatures from those by the legitimate card-holder suffering from fatigue.

Chemical eradicators allowed some card criminals to remove the legitimate signature from a stolen or lost card, and substitute their own. This made it necessary to overprint a signature strip with a light-colored pattern, using a special ink that would change color from contact with an ink eradicator. The ink would also rub off if any attempt was made to remove the signature with a rubber eraser. Another method is to print the word "VOID" repeatedly in the signature rectangle, and cover this with white ink which rubs off on contact with an eraser, exposing the warning.[2] Most of today's credit cards still use this method, as well as other security measures.

It's not necessary to erase the signature, as we'll see when studying methods of forgery. Spray paint covers the old signature, allowing the forger to write in his own version.

Check Digits

Each card has a unique serial number, consisting of several strings of numbers separated by dashes. Some groups identify the issuer. Another is the branch or office number. Yet another is the customer's account or identification number. Finally, there is a check digit or check number, based upon a formula, to enable a clerk to make a quick estimate regarding whether the card is legitimate. One way of generating the check digit is to add the month of the expiration date to the last number of the customer's serial number, and retain only the last digit of the sum. If the customer's account number is "62154," and the card's expiration date is "11/90," the check digit would be "5." If the expiration date were "5/90," the check digit resulting would be "9."

The check digit prevents a forger from altering a card by changing the expiration date, as he might if he rummaged through trash cans to find expired cards. It also prevents the most skilled forger from generating a card from scratch.

BIN Number

This is the "Bank Identification Number," and is a quick and dirty security check used in telemarketing transactions. The first four digits stand for the issuer company, and the telemarketer asks the telephone customer which bank or company issued his card. If the name doesn't match the BIN number, it suggests that the client is working from a charge slip carbon. The new VISA cards have the BIN number printed above the embossed one, and micro-printed as a frame around the VISA symbol.

Embossed Numbers

One way of making the card itself harder to forge or alter is to use a special laminate with a thin outer layer that peels away under pressure. Each card has a unique serial number, and a machine uses dies to emboss the number into the plastic. The raised numbers are different in color from the card surface, because the embossing has disturbed the outer layer.

Fine Line Printing

This is a repetitive pattern composed of fine lines printed close together that makes reproduction very difficult. One example is the blue panel on the right side of the VISA card. A pattern of fine black lines printed close together tends to burn out upon reproduction, while a pattern of fine white lines on a black background tends to "plug," or fill in. A fine line pattern combining both is practically impossible to reproduce without very high-resolution graphic arts techniques. For all practical purposes, fine-line printing defeats copying machines and most photographic reproduction methods, such as Polaroid cameras.

Micro Printing

This is extremely small printing, too small to read with the naked eye, and is very difficult to copy or reproduce by technical means. Without a magnifying glass, a line of micro-printing looks like a solid line. It reproduces as a solid line in a copy machine.

Ultra-violet Ink

Some checks and credit cards have images or symbols printed in ultra-violet ink. These are invisible to the eye in normal light, but show up very clearly under ultra-violet. The dove symbol on current VISA cards is printed in UV in the center of the card.[3]

Watermarked Paper

This is a method of making primary and supporting documents harder to forge. It has some value in protecting gift certificates, which as we'll see are often easy to duplicate or forge.

Metallic Ink

This is very valuable for making supporting and primary documents, such as gift certificates, harder to forge. Although there are toners of various colors available for office copiers, no copying machine uses metallic toner.

Photo I.D.

This is a system that didn't become popular, for various reasons, although other forms of I.D., such as drivers licenses, today carry a photograph of the licensee. One

problem is that a photo doesn't help at all when a customer operates an automatic teller machine.

Personal Identification Number

The personal identification number, or "PIN," is one way of ensuring that the person presenting the card is the legitimate cardholder. The card has an embossed number, and a magnetic stripe containing account and personal information. When the customer first receives his card, he selects a PIN, which may be numbers, letters, or both, and punches it into a keypad to record it in the bank's central computer. He's cautioned not to write his PIN anywhere, especially not on his card, and to select a PIN that won't be immediately obvious. PINs based upon name, birthday, address, social security number, auto plate number, etc., are too easy for someone else to guess.

In use, the cardholder inserts his card into the slot on an automatic teller machine, which prompts him for his PIN after reading the card. The customer punches in his PIN on an alphanumeric keypad, and the central computer matches his keystroke sequence with the PIN he recorded the day he applied for the card.

Stolen Card List

The "hot list" used to be very common, requiring each sales clerk to leaf through a booklet containing thousands of numbers of cards that had been lost or stolen. This method was only partly effective, for several reasons. First, new hot lists came out only weekly or monthly, providing a card fraud artist a grace period in which to work. A fraud artist with a little common sense would easily understand that, if he stole a credit card within a few days of the publication date of the hot list, the report would miss that month's list and he'd have an entire five weeks during which he could run wild with the card.

Another problem was that overworked clerks, harried by long lines of customers, would often miss a number listed in the booklet. Others would not even check, having become over-confident because they'd never yet accepted a bad card for payment.

Holograms

These are small metallic oblongs, containing a laser-etched image on their surface. The image changes shape and color depending on the viewing angle, and is very difficult to forge. However, there is now available a machine to apply holograms to credit cards. With a $17,500 price tag, this machine isn't cheap, but for the serious forger, it's not totally out of reach.[4]

Magnetic Striping

Painting a stripe of magnetic ink on the back of a card allows recording information that only a magnetic reader can read. Using non-standard stripe width makes it more difficult for a forger to encode information onto the magnetic stripe. Although it's technically possible to remove a magnetic stripe from a card and replace it with another, or to re-record over it, in practice it's uneconomical.

The American Bankers Association has a published standards for stripe characteristics and encoding language. ABA Document 1.2 deals with physical standards for credit cards, and the way the electronic data are encoded on the tracks in the magnetic stripe. ABA Document 2.8 deals with quality control. Both are available from the ABA or a bank, but not simply upon request. These are restricted documents.

Microprocessors

The "Smart Card," with a micro-chip embedded in the plastic, is the latest step in making credit cards secure

against forgery or misuse. The micro-chip contains much more data than a magnetic stripe, making it possible to maintain the client's entire account history on the chip. It can also hold a full description of the legitimate card holder, as well as special identifying information, such as a PIN, mother's maiden name, birth dates of his family members, etc.

In practical application, inserting this card into the slot of a card reader brings up a series of prompts. The screen presents questions which presumably only the legitimate card-holder can answer, making it extremely difficult for any unauthorized person to use the card.

Sources

1. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #7, July, 1984, p. 2.
2. *Counterfeit Credit Card Methods Exposed,* Carl Dorski, Keego Harbor, MI, Roadrunner Publications, 1979, p. 12.
3. *How To Protect Your Business,* Neil W. Sandler, Elmsford, NY, The Benjamin Company, 1985, p. 113.
4. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #8, August, 1984, p. 5.

4

Credit Card Forgery

In this chapter, we're going to look at document forgery from several different viewpoints, because forgeries are for different purposes. We have to look at the task facing the forger who is a total "outsider," and who must forge cards from scratch. We will also study how being an "insider" makes the task much easier. As we'll see, those with access to restricted materials and tools have an easy job of generating forgeries that will pass the most intensive examination.

In the early days of credit cards, forgery was fairly easy, because printing and security techniques were primitive. As we've seen from studying the security measures used to make credit card forgery difficult, creating bogus cards from scratch is extremely expensive and difficult. That's the way it should be, according to bank and credit card company security specialists. High-tech features, such as magnetic stripes and holograms, have made it uneconomical to forge credit cards from scratch.

Altering existing credit cards is somewhat easier, depending on the degree of alteration required and the level of scrutiny the forgeries will receive. Altering a credit card to serve as a primary document is still difficult, but if it serves only as a check guarantee card or secondary I.D., it's a lot easier. As we'll see, forging supporting documents is often the easiest of all.

For certain limited purposes, forgery can be cost-effective. An example is to make a check-cashing card, which doesn't need a magnetic stripe, or to use the forged card as identification for other purposes, such as opening a bank account under an assumed name. Supporting documents are also worth forging, if they don't have to pass scrutiny and it's cost-effective in time and materials.

Cost-effectiveness is the key. There's no point of spending many thousands of dollars to forge a credit card that can bring a return of only a few hundred dollars.

This chapter is not a hands-on teaching device to explain forgery step-by-step. There are other sources for this, all available on the open market. Equipment manufacturers provide instruction manuals with their equipment, and textbooks on graphic arts are for sale in many bookstores and available in almost any public library. Vocational high schools and community colleges teach graphic arts, and have shops where students may obtain hands-on experience in reproduction techniques.

Materials

Plastic sheeting is available from a plastics distributor. Hobby shops stock small amounts.

If the right color or thickness of plastic sheeting is unavailable, it's possible to simulate it by painting thin cardboard with spray plastic paint. Plastic paint is available in hobby shops, and is normally used to paint model aircraft and ships.

Tools

A basic tool is a silk-screen kit, used to paint logos and lettering on a plastic card. Silk-screening is a low-tech, low-volume way of producing good quality printing on cards, and requires minimal skill. Silk-screen kits are available at art supply stores, and graphic arts supply dealers. Prices start at about twenty dollars.[1] It will probably be necessary to buy extra ink, as the inks which come with the kit, if any, are not likely to be the necessary colors.

The starting point in silk-screening is a film positive of the subject. Because many credit cards are printed in more than one color, it's necessary to have a film positive of the artwork in each color. These are called "separations." To generate these separations, it's necessary to contact-print them from film negatives, made with a process camera.

This is a possible problem, because process cameras are very bulky, very expensive, and available only from graphic arts dealers. They also require skill to operate. While it's possible to go to a graphic reproduction shop and order negatives and film positives of credit cards, this might arouse unhealthy curiosity. A printer shows no curiosity about the legitimacy of a printing order, such as letterheads and business cards. However, a graphic technician may wonder why walk-in trade needs separations of credit cards, when he knows that credit card issuers have them commercially printed in large quantities. This is a stumbling-block that can trip up the amateur forger.

It's possible to improvise with a smaller camera, to avoid making strangers aware of the operation. A "view" camera, or a "press" camera is the starting point. A second-hand "Speed Graphic," will serve the purpose well. These use sheet film, and the smallest sizes are 2¼" x 3¼", quite large enough to make same-size negatives of credit cards. However, the most common size is 4" x 5", and these are often the least expensive, because they're fairly common.

The Speed Graphic is a press camera of obsolete design, and because it's outdated, is obtainable for one or two hundred dollars for one in good condition. A solid tripod or copy stand is essential. It's possible to improvise a copy stand, but the critical requirement is that the film plane must be parallel to the material being copied. A bubble level is a useful tool for assuring this.

One film to use is Kodalith Ortho Type III, available in 4" x 5" sheets from a graphic arts supply dealer. This film is not red-light sensitive, which makes it possible to handle using a red safelight for illumination. Loading sheet film holders is easier if the operator can see what he's doing. Developing the film is also easier under a safelight than in total darkness. The developer is Kodak Kodalith developer, or a similar high-contrast graphic arts developer.

The simple way to make film separations is to shoot a negative for each color, and to mask off the unwanted areas. This allows making a contact positive for each color.

Kodalith film is versatile, and the same box of film serves for both negatives and film positives. A contact frame is necessary for making film positives, and a simple high-intensity light provides enough illumination. For maximum sharpness in contact printing, the bulb should be at least five feet above the contact frame. The room walls should also be black or deep red, to avoid reflections that scatter light and cause it to strike the film at an angle. If this isn't possible, the bulb should be in a housing that shields the walls from direct light, allowing the light to travel only downwards onto the contact frame.

Another basic tool is an embosser for generating numbers on a plastic card. Embossers are available from business machine dealers.

Small magnetic printing machines are now available, but they're costly.[2] Obtaining the machine is only the first step. Devising the code to print on the magnetic strip is another problem, and this requires inside information.

Altering a credit card can be easy or difficult, depending on which features the forger needs to alter. It is possible to press embossed numbers flat with a soldering iron, and to emboss new ones, but it's easier to change one digit. Altering raised numbers almost always leaves traces, such as irregularities in the surface or texture.

The easiest thing to alter is the signature strip. As this has a special ink base, it's not worth trying to use ink eradicator or an eraser on the existing signature. Instead, the practical way is to paint over the signature with a matte spray paint, after masking the rest of the card with masking tape. If there are bank symbols or words overprinting the signature panel, it's easy to reproduce these with silk-screening. In many cases, though, a sales clerk won't even notice if these symbols or words are missing. It's possible to pass a plain background on a signature panel because the focus of attention is the signature itself.

For quick copies of credit cards and supporting documents, such as driver's licenses, a Polaroid film back is available for the Speed graphic and other 4" x 5" sheet film cameras. This is the Polaroid Type 545 film back, which accepts single film packs, in black and white or instant color, and adapts to any camera with a spring or Graflok back. This sells for about $200 at a professional Polaroid dealer, or graphic arts supply dealer.

This is useful for making passable copies of drivers licenses for use in situations which won't involve close examination. A lost, altered, or stolen driver's license serves as the base for the copy. Dropping altered information into the spaces on a genuine license allows the forger to give himself a new name, address, and even license number. Another way is to drop a new photograph into a stolen license.

No Polaroid copy of a drivers license will pass a police officer's scrutiny, even in poor light, but for casual I.D.

purposes, a Polaroid copy is perfect. Renting a mail drop is one use. Credit card frauds require a street address, and mail drop operators require some form of I.D. when renting a drop. They don't scrutinize the license closely, and copy information from it only because this is required by postal regulations. Likewise when a retail clerk asks for "two forms of I.D." to accept a check. The clerk isn't going to inspect each document to ensure that it's genuine, especially when there are other impatient customers in line. The fraud artist merely opens his wallet to the plastic card pockets, and allows the clerk to copy the license number and address.

A very easy document to forge is the drivers license learners permit. This is almost always a cheaply printed form, with no security features and no photograph of the bearer. A learners permit can often serve as a supporting document, because it is official paperwork.

A camera for large-volume reproductions is the Polaroid "MP" camera, which consists of the camera, copy stand, and lights. This is excellent for making reproductions, but it's a giant step up in price, costing thousands of dollars. The advantage of the Polaroid "MP" is that the operator can see the subject before pressing the trigger button, and easily adjust the scale of reproduction. This allows making half-size or double-size copies, which is sometimes necessary when making composites of other documents.

Probably the best compromise is a simple, fixed focus copy camera. One such is the Sirchie EVC-1000. This was originally designed as an "Evidential Fingerprint Camera," and it takes a Polaroid film pack to produce black and white or color prints. Its main advantage is that it's simple to use. It's fixed-focus, and reproduces at only 1:1. This is enough for making quick copies of drivers licenses or credit cards, if they're only for use as supporting documents.

It might appear that, with increasingly sophisticated technology, credit cards should become harder to forge. This is literally true, but at the same time we see another side of the coin. Retailers and even banks are accepting credit cards from many sources. A bank clerk may know exactly how to detect forgeries of the employer's cards, but cannot keep up to date on other issuers' cards. A clerk may not know that a certain issuer's card has a logo overprint on the signature panel, or has just changed ink color from blue to pink. This opens the way for the forger.

One type of primary document often very easy to forge or alter is the gift certificate. A credit card passer who chooses his target carefully can select a retailer who sells gift certificates printed on cheap paper in only one color. These are easy to alter or forge, especially if the paper has no distinctive watermark. Sometimes, simply duplicating the gift certificate with a copy machine is enough. If the certificate is harder to copy, adding a digit to the amount, to increase its face value, accomplishes the purpose.[3]

The "Inside Job"

By far, forgery of credit cards is most easily carried out by employees of the issuing company or the printing plant. These are high-security operations, with careful screening of employees, but occasionally an employee is tempted to go into business for himself, or put his talents to work for someone who will pay him more generously than his employer.

Traditionally, banks, credit card companies, and other financial institutions are stingy with their employees. They demand total honesty and loyalty, but are unwilling to pay for it with proportionate salaries and fringe benefits, except for the top rank of executives. This is why low-level employees who resent the disparity between the demands placed upon them and their salaries take advantage of op-

portunities to earn extra money on the side. One authoritative source identifies this as a major problem.[4]

Despite the controls placed upon credit card blanks, it's often possible to divert some because they're still blanks, and shortages often have other explanations. Once any card has an embossed serial number, it's more subject to control, and those who handle it are more accountable. Sometimes, however, an employee familiar with the control methods learns how to fudge the books to hide his diversion. In other cases, it's possible to conceal the shortage long enough for the employee to earn enough money to retire in another country.

The one commodity impossible to control is information. It's intangible, and impossible to lock in a vault. It's also impossible to prevent someone from passing it to another person. The employee with knowledge of security procedures and controls can sell his information, secure in the knowledge that it's impossible to prove that anything was stolen. Security officers examining the evidence of credit card fraud may suspect that an employee passed confidential information to unauthorized persons, but proving it is something else. The only leverage they have is to require an employee under suspicion to undergo polygraph examination, but this is an unreliable instrument. The suspect who keeps his cool can often manage to "beat" the polygraph.[5] Another problem with the polygraph is the increasing restrictions upon its use mandated by the federal government and various state legislatures.

One ring of "insiders" did get away with it, although their "outside" partners did not. In 1983, in New York, 11 people faced charges relating to counterfeit credit cards. They had obtained the numbers for the counterfeits from bank employees eager to earn extra dollars.[6]

During early 1989, the Bank of America in San Francisco uncovered a plot by insiders who had access to PIN

numbers. These people had planned to use the numbers, in conjunction with bogus bank cards, to withdraw money from the bank's ATMs.[7]

The printing plant employee has a far easier task. Diverting cards is simplest before they're numbered and put into a system of accountability. Some printing plants with high-security contracts use security measures right from the start, with a system that requires two signatures for every operation or transaction, such as counting card blanks. This may make it difficult or inconvenient to divert card blanks from a production run. But there are other ways.

Setting up any printing job always generates scrap. The press operator who wants to divert some cards only has to drop them into the scrap barrel and recover them later. For some purposes, genuine scrap will do very well. If it's not necessary to try to pass the card itself, an imperfect product will do. If the user needs the card only to support another transaction, top quality isn't necessary. This is especially true if a clerk will be merely copying the information from the card while it's still in the plastic window of a card wallet.

Two employees of a company in Maspeth, New York, realized that they could earn extra money by diverting some of their company's products. The plant embossed credit cards, and these two sold 1,500 cards, duplicates of legitimate accounts, to members of an organized crime ring.[8]

One highly-organized ring in Los Angeles made "credit kits" available to underground buyers. These were counterfeit credit cards and supporting documents, which were backstopped with fake credit ratings by dishonest bank, department store, and credit company employees. These insiders would alter company files to make the counterfeit cards appear genuine.[9]

The Real Fake Documents

Some printed documents, such as gift certificates, may be too difficult to forge economically. This can happen if there are watermarks, fine-line printing, metallic inks, etc. All of these impede copying, by photocopy machine or with a process camera.

A solution is to obtain stock printed forms, and overprint these with the required type. A totally fictitious entity, such as the "Main Avenue Merchants' Association," can serve for the ostensible issuer of the real fake document. Another way is to use a different printed form, overprinted with the lettering of the particular merchant, and pass this as the genuine article.

Another type of document is the legitimate "fake" I.D. Some small companies specialize in producing realistic-appearing I.D. cards that are purposely made to resemble genuine I.D. but without being exact likenesses. This makes these pieces of fake I.D. legal to sell, and even legal to use, as long as the bearer does not use them for "fraudulent purposes."

The bottom line appears to be that it's not worth the trouble for a credit card fraud artist to go to the trouble of forging cards. Genuine cards are so easy to obtain, by theft and subterfuge, that forgery is doing it the hard way.

Sources

1. *Counterfeit Credit Card Methods Exposed,* Carl Dorski, Keego Harbor, MI, Roadrunner Publications, 1979, pp. 22-23.
2. *Ibid.,* p. 28.
3. Associated Press, December 23, 1989.

4. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #5, May, 1984, p. 2.
5. *Interrogation,* Burt Rapp, Port Townsend, WA, Loompanics Unlimited, 1987, pp. 105-109.
6. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #5, May, 1984, p. 1.
7. Associated Press, December 29, 1989.
8. *Charge It!,* Terry Galanoy, New York, G. P. Putnam's Sons, 1980, p. 152.
9. *Ibid.,* p. 147.

5

Credit Card Frauds

There are many ways of using credit cards illegally but few, as we've seen, involve outright forgery. The tremendous number of valid credit cards in circulation makes it easy to obtain one by other means, without the technical expertise forgery requires. Credit cards are so widely accepted in this country that people lay themselves open to victimization because they use credit cards in everyday life.

Methods of Operation

The credit card passer, like the rubber check artist, normally follows certain guidelines, designed to enhance his credibility with cashiers. He knows that there are certain conventions upon which merchants insist, and he tries to blend in with the crowd.

The first step is reconnaissance. The professional card passer seeks to find the easy targets, and for this he'll enter various stores to observe their procedures. He may make small purchases himself, with cash or a legitimate card, so that he can see for himself whether cashiers ask for additional I.D. when a customer pays by credit card, and what sort of I.D. passes in a particular store. The professional also seeks out careless, tired, or inexperi-

enced cashiers, because these may be lax in security procedures.[1]

Another important factor is timing. The bad card passer needs the anonymity of a crowd, and knows that long check-out lines keep cashiers under pressure. This works in his favor, especially if the merchant hires high-schoolers as extra help during peak periods.[2]

"Temporaries" are very vulnerable to card passing, because they lack both experience and commitment to the job. As temporaries, they earn less than regular cashiers, and the job is just a small stepping stone, not a career.

The first tactical point is to appear respectable. The credit card passer does not enter a store dressed in rags, or demonstrate a surly or vicious manner. He does his best to appear respectable and pleasant. There's another reason for this. Blending in with the crowd makes him or her harder to describe or identify later. It's difficult for a police officer to pin down a physical description when the cashier answers "just average."

The second point is to conform to normal requirements for card passing. Most merchants require that the customer sign the charge slip, and provide his telephone number. The credit card passer must have a false telephone number memorized, or be able to make up a false number on the spot and without hesitation. Some merchants require additional I.D. The bad card passer does not rock the boat by trying to get around these expectations.

Sometimes, the fraudulent credit card passer won't have adequate supporting documentation with him, but many merchants accept the card anyway. Indeed, many don't even ask for supporting documentation. The reason is that merchants know that most transactions are by honest people, and that checking each one out to the limit would slow down business and even perhaps alienate customers. Another reason is that credit card and check

transactions don't fill the register drawer with cash, which is a tempting target for armed robbers. Many merchants prefer to keep as little cash on the premises as possible for exactly this reason. Therefore, they want to accept credit cards with the least amount of fuss and bother, which leaves the door open for the fraud artist.

ATM Robbery

Figure 3

An old lady making a withdrawal or deposit at an ATM is a tempting target for muggers, who can now take advantage of electronics to get more than just what's in her purse.

One very crude, although very effective, method of withdrawing money from an automatic teller machine, is by coercing the cardholder to do so (see Figure 3). Some robbers prey on people making late deposits or with-

drawals, lurking around teller machines and accosting the first vulnerable person they see. One armed robbery team specialized in kidnaping and credit card extortion. In one instance, they waited in the parking lot of a gay bar until a client emerged. They forced him to drive to his bank in his own car, and had him withdraw the money in his account. Afterwards, they left him tied up on the seat of his car, parked on a side-street.

The foregoing example isn't unique. In Dallas, robbers forced a man to drive ten miles to his bank, withdraw $200, and then shot him. In Hollywood, a gang of four robbers shot a TV newscaster at an ATM. In Texas, robbers attacked three ATM customers, forcing two of them to make withdrawals up to the $500 limit.[3]

This is why many ATM cards have limits on daily withdrawals. This prevents a robber from looting the entire account at gun-point.

Lost and Purloined Cards

Lost wallets are commonplace, especially in large cities, and many people on the fringes of criminality keep their eyes peeled for wallets, purses, etc., because they know that they can sell these to criminal contacts for the I.D. contained within. A set of I.D. can bring more money than a credit card, especially because I.D. does not become obsolete as quickly as credit cards, when their owners notify the credit companies of their loss.

Pick-pockets also do a brisk trade in wallet contents, after stripping the cash. Some prostitutes specialize in robbing their clients after sex.[4]

Some thieves work vacation resorts. They know that many vacationers carry credit cards as well as cash, and they wait until the victims leave their wallets behind: they raid their rooms when the vacationers are in the swimming

pool. Cash is always negotiable, and credit cards can be "wholesaled" off to a receiver.[5]

Mail theft brings credit cards, as well as various types of checks, and sometimes even cash. There are two advantages of stealing credit cards from the mails. One is that the card has a blank signature strip, and the illicit user simply signs the name on the card in his normal manner. This avoids problems in trying to duplicate another's handwriting. The other is that the legitimate card-holder doesn't become aware of their loss as quickly as he would become aware of a lost wallet. This gives the illicit user a grace period that can be several weeks long, before the credit company cancels the card.

Credit card issuers try to impede mail theft by various subterfuges. The principal one is to use envelopes with unrevealing return addresses. These are typically post office boxes, without the name of the bank or credit card company.[6]

Credit card issuers also avoid making it obvious that an envelope contains credit cards. One technique is to pack the cards in with a piece of cardboard, to prevent the distinctive shape from showing. Another is to vary the size and shape of the envelopes, as well as the return addresses, to confound mail theft. Actually, none of these precautions are worth much, because anyone legitimately receiving credit cards quickly learns the type of packaging, and credit card passers also have legitimate cards issued to them.

Postal clerks know which envelopes contain credit cards.[7] A dishonest postal clerk can earn extra money with little strain, and little risk, because of the general disorganization of the postal service today. Mail passes through so many hands, and so much of it goes astray in the normal course of affairs, that it's an almost impossible task to track down a few missing cards. Postal inspectors can pin it down only if the amount is very large.

Some cases begin as burglaries, or inside thefts. A burglar can make off with checkbooks and credit cards. A room-mate can abscond with credit cards and checkbooks, and the victim may remain unaware of the far-reaching effects of the thefts until the checkbook or credit card statement comes from the bank or credit company.

College towns occasionally experience rashes of such thefts. Students are not always as careful as they might be in selecting their room-mates.

ATM cards are especially vulnerable for several reasons. One is that bank statements come only once a month. Another is that, although banks set a daily limit on withdrawals as a protection against use under duress, a card passer who retains the card for an entire month can clean out the account.

It isn't even necessary to know the PIN to make withdrawals. A machine withdrawal requires the PIN to be punched in before the transaction can proceed, but the bearer of the card can make a pen and ink withdrawal slip transaction at a bank window. Because the card is accepted as proof of legitimate access to the account, anyone who has the card can make withdrawals. Although there is a signature panel on the face or rear of each ATM card, anyone who intercepts a card can insert his own signature.

One such incident occurred in San Francisco, beginning in 1986. A doctor's secretary intercepted his ATM card, and milked his account of about $15,000. An aggravating factor was that the doctor did not scrutinize his statements closely enough to spot the discrepancies, and the bank refused to cover most of his loss.[8]

There are about 80,000 ATMs today. ATM frauds amount to about $135 million per year, according to one estimate.[9] The amount may be much higher, but nobody who knows for sure is releasing the information. Banks keep any information on such thefts very close to the vest, because it exposes the extreme weakness of the system.

One type of ATM fraud which is no longer possible is collecting on a fake deposit. Automatic teller machines accept deposits, and credit them to the account. However, withdrawal of these funds is only possible after verification. Any card-holder can deposit an empty envelope, punching in whatever figure he wishes for the amount of the deposit. Likewise, a check may be the deposit, but the funds are on "hold" until the check clears. If the check bounces, the amount does not end up credited to the account.

Direct Merchandise Frauds

A very common type of credit card fraud is the "direct merchandise" method. This sort of operation is typically carried out by someone who is not a hard-core thief. Often, a juvenile will charge goods and services to a parent's credit card. One California couple found that their son had used their ATM cards and PINs to withdraw more than $2,000 from their account. In another case, parents allowed their son to use their ATM card to gain access to the family account, but later withdrew the authorization. They did not, however, change the card number or PIN.[10] One reason this practice is so common is that many people lend their credit cards to others, encouraging them to use them for their own purposes.[11]

A variation is the divorce-related buying spree. A wife, angered by an impending divorce, goes on a wild shopping spree with a card belonging to a joint account, knowing that her husband will be stuck with the bills. It's practically impossible to bring criminal charges against this sort of person, because a joint account is exactly that, and a vengeful wife can legally tap into the account all she wishes. Unless the husband has the foresight to clean out and close the account before the relationship goes critical, the wife can harass a financially strapped husband with more bills than he can pay.

In one case in Chicago, the wife ran up $15,000 in charges, to break her husband financially. As this amount was well over his annual income, her scheme worked. The husband had to give up the house, sell his car, and reduce his standard of living to the poverty level. The effect upon his mental stability was so profound that he couldn't hold on to his job.[12]

Merchants may accept the return of some goods, and this may help relieve the pressure on the victimized husband. However, if the charges were for services, such as dinners or airline tickets, the creditor is unlikely to forgive the debt.

One fact that some husbands don't realize is that their check cashing cards may also include a line of credit, allowing overdrafts. The bank will, of course, collect interest on outstanding balances. The vindictive wife may work the line of credit to the limit, both to secure ready cash and to cripple her husband financially.

The professional card passer understands a few basic tactics to avoid getting caught, and to avoid having his card questioned. First, he understands that many merchants still don't have point-of-sale terminals, and that with these merchants, it's possible to run up many transactions as long as they're under the floor limit. Keeping purchase amounts lower than fifty dollars will avoid setting off alarm bells for days. Likewise, it helps to have a friend or confederate working in a store or bank, to pass the word when the card becomes "hot." This allows using the card beyond the usual initial "safe" period.[13]

Fraudulently Obtained Credit Cards

Forgery is becoming less attractive, partly because it's so technically difficult. In any case, it's unnecessary, because banks and credit card companies are so eager to

hand out cards to almost anyone who files an application. This opens the door to fraudulent applications.

One way fraud artists obtain real credit cards is by taking advantage of the proliferation of applications in circulation. Banks and credit-card companies are so hungry for business that they even send pre-approved applications to their clients and others whom they consider good credit risks. With many applications dropped into the mail automatically, it's inevitable that some wind up in hands other than the addressee's. Anyone who moves, leaves an old address behind in somebody's records. Months or years later, if a credit card application arrives, someone else can fill it out, and receive a perfectly valid card in the other person's name.[14] We'll see later that this is a very common, and very successful, tactic.

Filling out a completely fake application is another tactic that works more often than banks and credit card companies want to admit. The 14-year old who obtained an American Express card by claiming that he was a 41-year-old doctor is one example.[15] The reason why this works so often is that banks and credit-card companies make the same mistake in processing card applications as they do in processing employment applications. They are reluctant to check out references thoroughly. Some feel that the losses thus incurred are still lower than the extra cost of thorough background checks.[16]

Another way is to pick up discarded credit card slips and carbons, and contact the bank or issuer, asking for a new card to replace one that was lost or stolen. The fraud artist also files a change of address, using a mail drop, to make sure that the replacement and subsequent statements come to him and not the legitimate owner. This delays discovery that the card is bogus.[17]

There have been several "classy" ways in which credit card passers have "trolled" for numbers, names, and addresses to use in fraudulent applications. One simple

way to build up a list of credit card holders, complete with their names, addresses, and credit card numbers, is to run fake advertisements soliciting mail or telephone orders. A mail drop or "boiler room" serves to collect orders. Upon receipt, these go into a file, and after a few weeks, the operator shuts down the operation. There's no cause for complaint by customers, because they do not get charged for any merchandise. However, the file serves as a basis for several types of rackets for the operator. He can order merchandise from legitimate telemarketing firms, apply for other credit cards, etc.[18]

Another fraud artist set up an "executive resume service," operating in several cities, offering prepared resumes at bargain prices. This procured for him the names, addresses, and other vital data about many real, established people, information he later used to fill out fraudulent applications for credit cards.[19]

Telemarketing Frauds

The rise of "telemarketing" sales has brought about another class of frauds. Telemarketing firms typically advertise their goods on TV, and urge the customer to phone an 800-number to place his order. Sales companies which accept credit card numbers over the telephone lay themselves open to frauds. The fraud artist never has to steal a card, as he gets the information he needs from a charge slip carbon picked out of the trash. He orders the merchandise, giving the address of a mail drop, and waits for delivery. By ordering a large quantity of goods, he can amass enough to be worth "fencing" through a professional stolen goods receiver.

One fraud artist turned out to be a bit of a practical joker. He placed 879 different orders for merchandise to be shipped to P.O. Box 787, at Lukeville, Ohio, the address of the state penitentiary.[20]

Another way of obtaining credit card numbers is by eavesdropping on conversations of people using cordless phones. This is a theoretical possibility, suggested in the August, 1984, issue of *Fraud & Theft Newsletter,* but it's probably not economical. The volume of telephone calls to monitor is simply too great to allow eavesdropping in the hope of picking up a call to a telemarketer.

One reason telephone marketing fraud is so successful is the greed of telemarketing companies, trying to get all the business they can. In the words of the *Frauds & Theft Newsletter*:

"Marketers are desperate to bring in new business. They are riding the rail trying to beat the competitor in getting the merchandise out before the ink dries on the check endorsement or the charge slip. Risky business because the thief writing a bouncing check or charging on someone else's credit card number gets the same super service as the honest customer."[21]

Careful selection of goods helps increase its value. The problem with some merchandise is that each unit bears a serial number, making it possible to trace. However, many small appliances, tools, inexpensive cameras, etc., don't carry serial numbers, and this makes it easier for the "fence" to insert them into his clandestine pipeline.

One development in telemarketing fraud has been the exploitation of telephone florists by a ring of male homosexuals. This variant is to order flowers by telephone, for delivery to their lovers, who then disclaim any knowledge of the sender. This is effective for several reasons. One is a Federal Trade Commission ruling that allows the recipient of unordered merchandise to keep it without any obligation to pay for it. This ruling originally was to prevent businesses specializing in high-pressure sales tactics from foisting merchandise on unwilling clients. As dishonest people have discovered, it also shelters the partners in third-party frauds.[22]

This type of scam isn't limited to homosexuals. Other fraud artists order merchandise delivered to a confederate, who then claims he never got the goods. This results in a charge-back to the retailer. This scheme is very popular for several reasons. One is that the con artist uses a genuine credit card, thereby avoiding the risks involved in using stolen or forged plastic. Another is that deliveries are sloppy, especially during the Christmas rush. Certain parcel delivery services don't require signatures for each delivery. Harried, overworked drivers, struggling to run their routes, are unwilling to return later, when someone might be home, and often leave packages at the door. This lack of control makes a claim of non-delivery very credible, and the con artist takes advantage of this.

Yet another reason is that police and federal agents don't pursue small cases. Credit card fraud artists know that they can get away with small thefts, amounting to only a few hundred dollars, because many public prosecutors won't bother to file charges on small cases.

Conversion Frauds

A fence isn't necessarily part of the picture. There are ways of converting purchases into cash without working through a fence. Fences never pay the criminal full value, because they have their own distribution expenses, and often have to dispose of the goods at lower than wholesale prices. A rough estimate is that the criminal who deals with a fence gets about ten percent of market price, although some authorities report conversion values as high as 35 percent.[23] This is a strong financial incentive to find another way of converting a credit card purchase into cash. For the credit card passer, there are many ways.

The individual enterpriser can make purchases for the purpose of obtaining refunds when he returns the goods. In many cases, this doesn't work because merchants mark

receipts and sales slips with "MC," "AMEX," or other appropriate notation to signify a credit card transaction. Upon return of the goods, they won't give cash refunds to credit card purchasers, instead filling out credit slips on their cards. This is why it's necessary for the credit card passer to break the chain, somehow.

One way is by buying airline tickets, if the purchaser exchanges the ticket for another one at another airline office. With a series of such exchanges, a clerk will eventually miss the notation that this was a credit card purchase, opening the way for a cash refund at the next airline office.

Another way is direct conversion of tickets to cash. One con man worked an airline ticket brokering system at the Oakland, California airport, purchasing airline tickets with a credit card at full price and selling them to passengers for cash at half-price.[24]

Another way of working this scam with merchandise is to return the goods for exchange, not refund. A con artist who buys an expensive camera or TV may return it to exchange for a lower-priced model. If store procedures are somewhat lax, the clerk may not notice that it was originally a credit card purchase, and refund the difference in cash.

A very practical and workable variant on the cash conversion principle is buying gift certificates with a credit card. A gift certificate is exactly like a check, in the sense that the bearer can obtain merchandise with it. There are some differences, however. The gift certificate is negotiable only with the merchant who issued it. It is more easily negotiable, as gift certificates are already paid for when redeemed. This is why many merchants accept their own gift certificates without question, and do not demand I.D. for the transaction. A practical point is that gift certificates are very common during the Christmas season, and over-worked clerks are unlikely to question their own stores' gift certificates.

It's even possible to sell the gift certificate on the street, obtaining a higher price for it than for stolen merchandise. By carefully selecting the merchant, it's even possible to cash in a gift certificate. [25] Another choice is to use the certificate for a purchase less than face value, and accepting the difference in cash. Finally, the fraud artist can return the purchase for a refund.

Auto Theft Via Credit Card

Credit cards are helpful accessories for auto theft. The car thief uses a stolen credit card to rent a car. With the rental agreement in the glove compartment, he doesn't have to worry about being stopped by a police officer. Another benefit is that the rental provides the thief a grace period before the rental company reports the vehicle stolen.

Telephone Company Credit Card Fraud

Another type of telephone-related fraud is illicit telephone company credit card use. As with telemarketing frauds, the perpetrator doesn't need the card itself, only the card number. A telephone credit card allows the bearer to make long-distance calls from literally any telephone in the country, including a pay phone. The weakness in this method is that the fraudulent user calls someone who knows him, and it's possible to trace the user by questioning the recipient of the call.

Merchant Collusion

Some credit card scams run with the cooperation of the merchant. At times, the merchant instigates the scam. The merchant accepts a forged credit card in payment for fictitious goods or services, then collects from the credit

company or bank. Making this scheme work successfully requires that the goods or services be untraceable. Trying to "sell" a phantom videotape recorder, for example, is difficult because of the serial number. A restaurant operator, on the other hand, has an easy time of it, because he sells untraceable commodities. Clothing and shoe stores, as well as merchants who sell other types of un-serialized goods, can use this scheme without fear of being traced.

Some dishonest merchants have other techniques of using credit cards for fraudulent purposes. One technique is "raising" a charge slip. This is basically the same method a check artist uses, raising the amount to a larger one. This works best when padding charge slips to company accounts, as private customers generally keep their charge slips and they know the amounts of their purchases. It works extremely well with gasoline purchases for company cars. If a company comptroller does not insist on employees' turning in charge slips drawn against company credit cards, they can't compare them with the statements, and are vulnerable to theft.

Another method is to stamp two or three slips, bringing only one for the customer to sign. The merchant now has a couple of blank slips, stamped with the customer's credit card stamp, and he fills these out for non-existent purchases. In one case, a network of dishonest restaurant cashiers routinely ran customers' cards through to make several charge slips. They used these slips to pad their cash drawer, covering withdrawals into their own pockets.[26] Again, this works best with corporate card purchases.

Another con artist "wholesaled" charge slips. This fraud artist, a waiter, took his clients' credit cards into the back room and ran off several charge slips on the imprinter. He sold these to others, who used them for various purchases, including a car.[27]

Kiting

Check "kiting," or writing a check to cover a previous check on another account, is illegal, because inevitably, the last check written will bounce. However, some strapped people are doing something like that with credit cards.

Some people, who can't resist the advertisements that promise the good life through the magic of bank plastic, find themselves in more debt than they can handle. With a slew of bank cards, and the easy payment terms that apply to these credit accounts, it's possible to obtain cash advances and use these to make the minimum payments. With time, this bubble will also burst, but by careful juggling with several credit cards, it's possible to postpone the moment for a long time.[28]

Bust-out

A connection with organized crime occurs with a "bust-out" operation. The organized crime operator buys out a legitimate company, and takes out legitimate corporate credit cards in that company's name. He uses the credit cards to pay for many goods and services, with the credit card issuer billing the taken-over company. After several months of milking this company's line of credit, the operator files bankruptcy.

Credit Card Processors

This category is fraud directed both against the bank and the consumer. During recent years, there have been advertisements directed towards people with bad credit, who would like to have credit cards. Various companies

have promised that they could dry-clean a person's credit record to allow him to have a credit card once more. The gimmick was that poor credit risks could obtain cards if they opened savings accounts with card-issuing banks to secure their line of credit. The companies would collect the money, retain it, liquidate the assets, and file bankruptcy before depositing any of the money with the participating banks.[29]

Another technique is that used by "credit doctors," who purge a client's credit records by obtaining the access codes to credit reporting bureau computers and deleting derogatory information from their files. However, this is only a quick fix, and not very helpful in the long run.

A more imaginative use of credit bureau files is to purloin the identity of a person with a name similar to the credit doctor's client, retrieve the information on that person, and relay it to the client to put on his or her credit card applications. This process can easily provide the client with a quantum jump in credit card limits, because the credit doctor selects someone with higher income or more assets.[30]

Gaining access to credit bureau records requires a computer with a modem and communications program, and the access codes. The credit doctor obtains the access codes from credit bureau employees, who are very vulnerable to monetary appeals. The reason is that credit bureaus, like banks, insurance companies, and other financial institutions, are very chintzy with salaries and benefits, except for the favored few at the top. Rank-and-file employees, however sensitive the information they safeguard, get the crumbs, and many resent this exploitation. When they find an opportunity to cash in on their specialized knowledge, some take it.

Another way to fix bad credit is to put a "hold" on the information by contesting it. Some credit doctors have a regular practice of sending letters contesting derogatory

information in clients' files to credit reporting bureaus. Federal law prohibits disclosing challenged information until the credit bureau resolves it with an investigation. This creates a grace period for the client, during which he or she can apply for more credit cards, loans, etc.

New Ways of Fraud

As we've seen, fraud and fraudulent obtaining of cards works better than forgery. The canny fraud artist isn't going to fight credit-card issuers on their own territory, producing cards, because he'll come up second-best. Instead, he'll use the system's weaknesses against it, to his own advantage.

Sources

1. *Small Business Security Handbook,* James Edward Keogh, NJ, Prentice-Hall, 1981, pp. 101-102.
2. *How To Protect Your Business,* Neil W. Sandler, Elmsford, NY, The Benjamin Company, 1985, p. 108.
3. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #8, August, 1984, p. 3.
4. *Counterfeit Credit Card Methods Exposed,* Carl Dorski, Keego Harbor, MI, Roadrunner Publications, 1979, p. 3.
5. *Charge It!,* Terry Galanoy, New York, G. P. Putnam's Sons, 1980, p. 150.
6. *Credit Card Fraud Control Manual,* American Bankers Association, p. 23
7. *Charge It!,* p. 149.
8. *Los Angeles Daily News,* February 5, 1989.

9. *Ibid.*
10. *Ibid.*
11. The author, who earns a living as a free-lance writer, was recently given a telephone credit card number by one of his editors, who told him to use it for calls made relating to articles for his publication.
12. *Charge It!,* p. 178.
13. *Ibid.,* p. 149.
14. Knight-Ridder Newspapers, May 15, 1989.
15. *Fraud & Theft Newsletter,* V. 2, #2, February, 1984, p. 8.
16. *Charge It!,* pp. 200-201.
17. *Ibid.,* pp. 149-150.
18. *Ibid.,* p. 152.
19. *Ibid.,* p. 152.
20. *Ibid.,* p. 151.
21. *Fraud & Theft Newsletter,* V. 2, #7, July, 1984, p. 1.
22. *Fraud & Theft Newsletter,* V. 2, #6, June, 1984, p. 7.
23. Associated Press, December 23, 1989.
24. *Charge It!,* p. 145.
25. Associated Press, December 23, 1989.
26. *Fraud & Theft Newsletter,* V. 2, #6, June, 1984, p. 7.
27. *Charge It!,* p. 146.
28. *Ibid.,* pp. 183-184.
29. Knight-Ridder Newspapers, May 15, 1989.
30. *Wall Street Journal,* August 14, 1990.

6

Consumer Victimization

The decade of the eighties has shown, perhaps more clearly than any previous period in American history, the true motivations and immoralities of major financiers. Stock market manipulations, "insider" trading, "junk bond" deals, and the savings and loan scandal have been the tips of several icebergs. In reality, several other schemes have been going on for even longer. The one which concerns us here is the systematic criminal exploitation of individual consumers by banks and credit card companies.

There's a long history of client exploitation by banks and other moneylenders. Until the "Truth in Lending Act" of the late 1960s, banks and finance companies used overly complicated charts and tables to prevent their borrowers from knowing the true interest rates they were paying. Other practices, such as late billing to force the customer to pay finance charges, were very common, until a spate of new federal laws made them illegal. However, it's important to remember who has greater influence over legislators: it's not voters, but those who make large campaign contributions. It's easier to cheat when you have a hand in writing the laws.

This is why the consumer must be doubly watchful. If he feels that the bank or credit card company has sandbagged him, he has no recourse to the police. They're not

on his side, because the bankers and businessmen write the laws. Although consumer protection laws in this country have improved greatly during the last two decades, they're still inadequate.

Many people accept as "normal" the charging of interest on any balance remaining after billing. This carries over until the next month, at the interest rate stipulated in the contract. However, it's also legal to charge interest from the day the charge is posted in the account, making interest charges inevitable for anyone using such a credit card. Another way is to charge a fee for every transaction. This may be from 10¢ to $3.00 for automatic teller services. Fully covered by the laws, bankers and credit companies play "Gotcha!"[1]

There are many ways, legal and not-quite-legal, in which bankers and creditors can milk their clients. Dishonest bankers have cheated their customers for years. The recent introduction of computers into the banking business simply makes it easier to do so, and affords the dishonest banker a convenient excuse, "computer error," if a customer complains.

It's also important to note that customer cheating may not be at the instigation of the bank or credit company management, but a corrupt employee. This is the high-tech equivalent of the short-change artist.

One way of generating extra income at a customer's expense is to omit sending the customer the bill, to generate interest charges which will show up on the next month's bill. This is extremely common, and even occurred on one of the author's doctor bills.[2]

Another way is to send out bills, but not enter credit for any payments made. This can work with people who are unsophisticated, or simply careless with their accounts. When the perpetrator is a large bank with millions of accounts, it's easy to generate many thousands of dollars of extra income this way.

An almost fool-proof method of cheating customers is to program the computer to notify the customer of any mistakes he makes, but not telling him of any the computer makes, as long as they're in the bank's favor. An overpayment, for example, brings extra revenue if the computer simply omits notifying the customer that he overpaid. If he underpays, he gets an immediate notification of the amount due, perhaps with an interest charge tacked onto it.[3]

Rounding off numbers is always profitable, if the computer rounds them off in the bank's favor. Likewise, the practice of "shaving" percentage points on interest appears to be small beer, but over the months and years it adds up to many dollars.

Fictitious charges are another type of dodge. Many people don't scan their monthly statements, and those who do may not worry much about an extra "service charge" of a dollar or two. It usually isn't worth taking time off from work to go to the bank to inquire about it. Even a phone call may not seem worth the trouble, for only one or two dollars. When this happens, the bank's done it again.

The credit consumer has every reason to be vigilant. His predators are not only credit card passers, but the banks themselves.

Sources

1. *Charge It!*, Terry Galanoy, New York, G. P. Putnam's Sons, 1980, p. 184.
2. On one occasion, the physician's billing clerk added a "finance charge" of 16¢ to the bill, which she later claimed was for charges accruing from a previous month, which had remained unpaid. She claimed to have mailed a bill, but the author never received it at

the time. Sixteen cents isn't much, but multiplied by one hundred patients, it adds up to sixteen dollars per month. If the patient doesn't notice the fraudulent charge, or doesn't complain, the billing clerk may increase it next month, and may even "pad" the bill by several dollars.

3. *Charge It!*, p. 119.

Part II

Tactics

Credit card fraud receives low priority from police agencies. As we'll see, the key to successful apprehension and prosecution is linking successive acts of fraud to form a pattern.

7

Police Response

Merchants who hope that their local police agency will vigorously pursue credit card fraud artists may be in for a surprise. Police agencies are overloaded, and non-violent crimes involving small amounts receive very low priority.

An additional problem is that much credit card fraud is across state lines. This is both good news and bad news. The bad news is that jurisdiction of local agencies is limited to intra-state crimes. A local sheriff or police department can't pursue credit card fraud conducted against telemarketing firms accepting orders from all 50 states, for example. Another problem is the mobile criminal, moving from state to state, and passing his fraudulent plastic everywhere he stops. It's very hard to catch up with the mobile passer, because he's already gone before the reports begin reaching police.

The good news is that interstate crime falls under the jurisdiction of the FBI and the U.S. Postal Inspection Service. Both of these agencies obtain convictions in well over 90% of the cases they bring to prosecution. The Postal Inspectors do slightly better than the FBI, although they're not as well-publicized.

Unfortunately, there are limits to their involvement. Postal Inspectors get into a case if it violates Public Law

93-495, the "Truth in Lending Act." Section 134 pertains to fraudulent use of a credit card, and applies to people who accumulate $1,000 or more per year in fraudulent credit card charges. It also applies to moving forged or fraudulent credit cards between states, knowing that the cards are forged.

Another problem is that, although these government police agencies have high success rates with cases they bring to prosecution, they don't take all cases to this stage. Indeed, one reason for their high success rates is that they choose very carefully the cases they pursue. Their directors understand the value of success statistics when presenting their budgets to Congress, and they aim to obtain as high a percentage of convictions as possible. The net result is that they don't pursue unpromising cases.

In practice, it's difficult to determine if the crime falls under the provisions of the act without a complete investigation. A credit card scam to obtain a rental car for theft is obviously within this limit, but by the time the rental company reports the car stolen, the trail is very cold.

Police investigators are often left far behind by experienced card passers who understand the system. One of their tactics takes advantage of the way police investigators think. Professional criminals know that police investigators, burdened with more cases than they can reasonably handle, often try to "clear" a large number by blaming them all on one individual they catch. This is the key to disposing of a "hot" credit card.

One way to do it is simply to drop it on the floor in a well-traveled public place. Anyone who picks up the card, and gets caught using it, will become the object of an intensive investigation, and will wind up being charged for

all frauds committed with that card. Another way is to sell the card to another member of the underworld.[1]

Even without direct evidence, such as signature comparisons, police officers will often try to arrange a "deal," whereby the suspect admits to a slew of crimes in return for a lesser sentence. This requires the collaboration of the prosecutor and the judge. They, too, understand how the system works, and usually cooperate closely with the police.

Sources

1. *Charge It!*, Terry Galanoy, New York, G. P. Putnam's Sons, 1980, p. 149.

8

Prevention

Credit card fraud, like most other crimes, does not involve the police at the start. Discovery of the crime may be many days or weeks after it occurs. As with other crimes, the citizen is the first line of defense.

Ordinary street crimes, such as muggings, burglary, and motor vehicle theft, can involve almost anybody. Credit card fraud directly involves only two parties: anyone who loses a card or has it stolen, and the merchant and bank who accept that card as payment. While there's not much hope of preventing credit card losses and thefts, because there are so many vulnerable points, there's reasonable hope of preventing some of the frauds because merchants and banks are concentration points. A credit card fraud operator can't victimize just anyone, as can a passer of counterfeit currency. He can victimize only those who accept credit cards as payment, or as supporting documents.

Giant financial companies, such as the systems which issue VISA and Mastercard, are taking steps to protect themselves. An information-sharing program, which cross-checks applications, went into effect in April, 1989. The system compares names, addresses, social security numbers, telephone numbers, and other personal identifiers, and flags those that match those on another card. This alerts the companies to possible fraud, in which a

card passer applies for several cards under different names.[1]

The reason this works is that card passers often do not create totally new identities to match the persona when they apply for different cards. Social security numbers, addresses, or telephone numbers often overlap, allowing a cross-match. We'll get more deeply into this in the chapter on information management.

Personal Alertness

Obviously, combating credit card fraud often begins with the card-holder, who should report immediately any loss or theft of credit card. As important is safeguarding his cards to reduce opportunities for theft.

Yet another step is watching carefully who uses cards. A parent who allows a son or daughter to use his or her credit cards may be buying trouble. Likewise, any man facing divorce should secure the credit card front before the main action begins.

Retail Precautions

Retailers deal directly with people, both their employees and clients, which makes the human factor the most important one in the equation. Hiring and keeping good people is an important first step which many employers neglect.

There are actually two important parts to staffing with competent people. The first is hiring. It's important to hire intelligent and honest people at the outset. Many small employers, however, chronically complain that "It's hard to find good hired help nowadays." Good hired help is always available, but at a price. Careful hiring helps ensure that you get what you pay for, but without adequate pay, the employer will soon find that he doesn't get what he's unwilling to pay for.

One important reason is that much advice on personnel practice concentrates on security, instead of good employee relations. One authority considers a thorough check on applicants necessary, because of the possibility of hiring undesirables.

Background Checks

All applicants fill out the same forms, listing previous employment, education, and personal data, but few employers bother to check out the information. Instead, they use paper-and-pencil "honesty tests" huckstered by fly-by-night "personnel screening" specialists, or they require polygraph examinations from their applicants and employees.

The purveyors of these screening tests are very quiet about one point: the failure or error rate. It's practically impossible to obtain any information from them regarding how often their tests fail to detect an undesirable applicant. Those who claim that their success rate is near 100% are liars. Most will, to avoid stating an outright lie, avoid answering the question.

The theory is that these techniques are short-cuts to securing good employees, and make background checks unnecessary. This is false economy. A skilled liar can fool an interviewer. Some people are very good at "passing" paper-and-pencil tests or polygraph tests. Only background checks can verify the statements made in the employment application, or the answers to the interviewer's questions.

A major point that many employers and interviewers miss is that the information contained in the application

and the candidate's answers to interviewer's questions must be verifiable. It should be possible to contact former employers to confirm the applicant's employment record. This is why the name, address, and telephone number of a contact person is essential for every employment listed. If any are missing, the interviewer should ask the candidate for them, making it clear that he intends to contact them. The applicant should also explain any gaps in employment history. Sometimes, gaps may reveal time spent in prison. A gap may also represent time spent at a job which the applicant doesn't want to declare because his former employer would have derogatory information.

It's possible to document many gaps. If the applicant states that he spent two years abroad, he should still have his passport, especially if it's still current. Some people keep even expired passports. The passport often shows exit and entry stamps, which confirm the applicant's story. If the applicant states that he took two years off to attend college full-time, he should have some paperwork to support this. Once he has the application and the candidate's statements, the interviewer should follow up and verify the references.

Occasionally, a reference will be unverifiable because the company has moved or gone out of business. This is normal, but an employment application which lists mainly businesses which no longer exist is suspect. So is one which lists foreign travel for which no documentation is obtainable.

An important point in checking references is to understand the "code," by which employers pass on information without making themselves liable to lawsuits by former employees. Because of several lawsuits against former employers who provided derogatory information and kept their former employees from obtaining jobs, companies are now reluctant to provide any information except to verify the period of employment. If a former employee was unsatisfactory, they simply refuse to provide any information at all. This is the code, which avoids the threat of lawsuits. This is why reference checking should be by mail and on the company letterhead, if time allows, both to show that the inquiry is bona fide, and to allow the other company the opportunity to decline to answer if the employee was unsatisfactory.

Keeping Competent Hired Help

A background check isn't enough. Hiring good people is not the same as keeping them. Employees who feel that management treats them fairly won't harbor the smoldering resentment that an exploitative relationship fosters. This is why it's important for the employer or manager to concentrate on the big picture, instead of the narrow view of one authority who describes security efforts in terms such as "putting pressure" on dishonest employees.[2]

Unwillingness to provide adequate pay and benefits doesn't really save money, in the long run. Instead, such a policy has several effects, some of which show up immediately, and others which appear later:

- Many qualified applicants lose interest in a position which pays less than that offered by another company. The competition hires them.
- Those who remain interested in the position are the duller and less qualified ones, including "losers" who drift from job to job. Such people have little motivation, because they know that low-paying, dead end, jobs are easily available.
- If the applicant for a low-paying job appears qualified, there are only two possibilities. He may accept the job only because of immediate financial need, and will be constantly seeking better employment. If he's got a reasonable amount of talent, he'll find it fairly quickly.

  The second possibility is more sinister. The seemingly qualified applicant has a hidden agenda, per-

haps seeking to become the "inside" man for a burglary ring, or he may be planning a series of small thefts to earn extra money.

- Poor pay and benefits lead to high turn-over. This causes the employer to spend more time interviewing and evaluating applicants, and training new hires. He can spend less time on other necessary functions, such as monitoring security.
- The employee who accepts the job in good faith probably will lack a sense of commitment to the company, because he's not planning to remain. He'll view himself as a "temporary," even though his employer may have hired him as a permanent employee. He may even be bitterly resentful, feeling that he's being exploited. He won't be giving "100%," and his main goal will be to get through the week without too much strain and blame.

Any employer who expects loyalty from his people must be willing to give it in return. An employer who lays off employees with two minutes' notice can't expect that his employees will give him two weeks' notice when they find other positions.

The enlightened employer who understands that loyalty is a two-way street will get more from his employees. If he pays well enough, he gives his employees a vested interest in keeping their jobs, because they'll know that they won't easily be able to find another position with the same salary and benefits. This builds a sense of commitment, and willingness to perform to keep the job. This includes observing security measures against credit card cheats.

Security at the Cash Register

There are several precautions a merchant and his employees can take to make life harder for the fraudulent credit card passer:

- Compare signatures on the card and charge slip. This is a simple first step, which although not fool-proof, will stop some frauds. It isn't fool-proof because a skilled fraud artist can paint over the signature strip on a credit card, and sign it himself. The professional obtains fresh, unsigned credit cards, and signs them before starting out on his rounds.
- Check the expiration date religiously. This prevents passing an expired card, which may have been picked up in someone's trash. This can also reveal a new card, and this is suspicious if the customer is making large purchases with it. The client may have just stolen it from someone's mailbox, and may be trying to make as many charges as possible on it before it becomes void.
- Look for signs of forgery or alteration. These may be:
  - ☐ Missing logos.
  - ☐ Chipped or peeling panels.
  - ☐ Warped plastic.
  - ☐ Erasures.
  - ☐ Alterations of the signature.
  - ☐ Printing on the outside of card's laminated surface.
  - ☐ Embossed name does not match signature.
- Ask for additional I.D. This is only a partial measure against professional credit card passers, because they come equipped with supporting documents. However, recording this additional information can help spot a fraudulent user with sophisticated databases. The reason is that, although a fraudulent user may change credit cards often, even daily, he's less likely to change his supporting documents often.
- Scrutinize the extra I.D. more carefully than the credit card, because this is where fraudulent credit card

passers try to cut corners. The photo and description on a drivers license may not match the bearer, for example. Another possible problem is the learners permit, which does not have a photo, as does a regular drivers license. It's also cheaply printed, and very easy to forge. The easiest form to forge is a federal firearms license, which is literally a photocopy of a cheaply printed original.

- Each charge slip should have the sales clerk's name or identifying number on it, for accountability. This pin-points efforts at collusion or double-charging by dishonest employees.
- Clerks should not ask their charge customers to write their telephone numbers on the charge slips. This merely makes it easy for the fraud artist who hangs around parking lots to pick up discarded charge slips and carbons.

The uselessness of asking for telephone numbers should be evident. In most retail outlets, nobody checks them. Even if a clerk or manager were to check each phone number with the directory, many customers would not check out, because they have unlisted numbers.

It's also helpful for clerks to watch for elements of the behavioral profile that signifies possible card fraud. Customers who appear excessively nervous, and who carry the card in a pocket instead of a wallet are worth watching. In a clothing store or department, so is anyone who buys clothing without trying for size, or refuses alterations included in the purchase price.

Some signs are very clear. A customer who asks the clerk to split the ticket to avoid the need for an authorization call is obviously trying to get away with something. So is a customer who asks about the floor limit.

Telemarketing firms should require their employees to ask for not only the card number and expiration date, but the bank name on the card, and to match it against the

"BIN number." This is the first four-digit group of numbers on a card, which stands for the issuing bank. This stymies the fraud artist who finds a charge slip carbon and tries to use that number, as the printer does not copy the bank name.

Obtaining a BIN number directory can be difficult, as some banks are reluctant to pass out copies.[3] The telemarketer must then compile his own, by asking each caller the name of his bank. As most will be truthful, it's soon possible to compile a small directory to verify other callers' cards.

A large merchant, such as a department store with its own security department, can afford a computer to monitor fraudulent activity. For most effective use, this requires a full-time staffer, but it can pay for itself by preventing fraud losses. One way is to compare credit card users with a list of fraudulent I.D.s used in the past. Another is to check for a pattern of sudden activity. A fraudulent card passer who works a department store will often hurry from one department to another, making as many purchases as possible in a short time, before the card gets "hot." Monitoring this sort of use can allow apprehension before the fraudulent user leaves the store.[4]

Prevention at the Source

The credit card issuer can also help prevent credit card frauds. A small amount of time and resources invested in this effort is very cost-effective.

Clerk Training

Merchants are stingy in employee training, as this is not an obvious profit center. Typically, merchants train their sales clerks to operate the cash register and fill out sales slips.[5] They often give little attention to security, other

than telling their clerks to ask for two pieces of identification when accepting checks. One way to fill this gap is for the card issuer to conduct seminars for sales and check-out clerks, at the merchant's place of business. A security agent can demonstrate proper security procedures to the employees, explain how fraud artists work, and answer questions. A display board, with samples of forged credit cards and supporting documents, is very helpful because it's more vivid and graphic than a simple description.

Forward-looking merchants ought to do this for themselves. Unfortunately, many merchants are stingy with pay and employee benefits as well as training time, and this keeps employee morale down. As we've seen, an employee who feels that the employer cares little about him or her is not going to make a great effort on the job, instead doing merely the minimum required to "cover" himself. The attitude is likely to be: "Why should I bother to protect the boss's money?"

Monitoring Credit Card Activity

Another way for the issuer to protect himself is to monitor credit card use very closely. This requires a special program in the computer that processes receipts. This can identify patterns of activity that arouse suspicions. For example, if the floor limit is $50, and there are many charge slips for $49, this suggests a pattern of collusion and fraud. Another alert sign is a sudden and unexplained increase in activity.

Credit charges tend to be seasonal, following the level of business. An increase before Christmas, for example, is normal with many retailers. However, an increase that seems out of place may be early warning of a take-over and bust-out, with the retailer filing many credit slips and running with the money before the fraud catches up to him.[6]

Another important point is to monitor activity on individual cards. A flurry of charges may be a signal that the card has been lost or stolen, and that the finder is trying to make as many charges as possible before the owner reports the card missing.

Electronic data processing is the only way of effectively catching some of the frauds before completion. The reason is that credit card fraud artists move quickly, and can easily charge totals far beyond the limits before they discontinue use of a particular card.

A printed "hot list" is outdated. It simply takes too long to collect and disseminate the information.

It's also important to monitor merchants for patterns of activity that may indicate fraud. Most individual signs are not clear-cut, because they often have other explanations. In every case, however, they're indicators for closer scrutiny.

- An unusual number of large authorizations may indicate a pattern of collusion for fraud. This is especially significant if there's a sudden build-up.
- Authorization calls made outside normal business hours for that merchant show that something unusual is happening. These may be late at night, or on holidays during which the business is not normally open.
- Several purchases on the same card, on the same day, should call for an alert. The exception is a department store, where it's logical for a customer to make several purchases, each in a different department.
- Daily cleaning out of the account is also a sign for suspicion. The merchant may simply have poor cash flow, and need every cent he can raise as quickly as it comes in, but this can also signify keeping prepared to flee. If the merchant cleans the account out daily,

it becomes important to know what he does with the funds. Does he take cash? Does he buy certified or traveler's checks? Does he deposit the money in an account at another bank? Close internal liaison allows a close look at canceled checks, if any, to show what sort of pattern is developing. Large fund transfers to what appears to be a shell company is often a first alert for fraud.

- Change of ownership is always cause for a closer look. This is especially true of a company with a very good credit rating. A takeover by a larger firm in the same field isn't sinister, but if the buyer is an unknown company, this could be the precursor to a bust-out.
- An almost unmistakable sign of fraud is a large number of charge slips just under the floor limit. This can come about because a fraudulent card passer makes repeated purchases under the limit to avoid the authorization hassle, but also because a merchant is trying to collect on fake sales, passing the charge slips to the bank for collection of nonexistent sales.

Closer scrutiny involves checking the business out with Dun and Bradstreet, and the Better Business Bureau, as a first step. It may also be revealing to run the names and addresses of the owners through the main database, because this may reveal a connection worth investigating.

Enhanced Authorization Services

One way to help squeeze down fraud is to offer additional information to the merchant who phones for an authorization. Providing the card-holder's address and telephone number allows the merchant to compare them with the address given by the client, or the address listed on supporting documents. A certain percentage of address mis-matches are legitimate, because people do change addresses from time to time, but the discrepancy can alert the sales clerk, who may then ask for additional I.D.

As we'll see in the information management chapter, a computer database can be extremely helpful in spotting names, addresses, and other personal identifiers which have been associated with fraud in the past.

Sources

1. Knight-Ridder Newspapers, May 15, 1989.
2. *Small Business Security Handbook,* James Edward Keogh, NJ, Prentice-Hall, 1981, pp. 47-65.
3. *Fraud & Theft Newsletter,* Boynton Beach, FL, Fraud & Theft Information Bureau, V. 2, #7, July, 1984, p. 4.
4. *Fraud & Theft Newsletter,* V. 2, #9, September, 1984, pp. 4-5.
5. *Fraud & Theft Newsletter,* V. 2, #3, March, 1984, p. 4.
6. *Ibid.,* p. 6.

9

Counter-Attack: Striking Back At Frauds

Apprehension and prosecution of credit card criminals is a hit-or-miss proposition in many cases, because this sort of crime takes low priority. However, with innovative thinking, and careful coordination, it's possible to work credit card cases as parts of larger investigations.

Cooperation Between Merchants

Small retailers cannot operate full-time security departments, but a merchant's association can, by pooling resources. In shopping malls, for example, the mall management operates a security department as part of the mall's service to its renters. Some neighborhood or area-wide merchant associations also provide various security services for their members.

A fraud case clearinghouse can bring together separate incidents of fraud to disclose a pattern. This helps in gaining the cooperation of the police. Collecting and disseminating information also serves to warn other merchants against particular fraud artists currently working in the area.

The security office that operates a central clearing house can also receive alerts from merchants who have spotted fraud artists, and can dispatch security agents to

observe and apprehend the perpetrators. A well-coordinated security program collects reports, correlates them, and prepares material for a prosecution.

Electronic Data Bases

The value of a computerized data base is to spot patterns, and to identify individuals who are repeatedly involved in fraudulent transactions, such as third-party frauds. A simple example is the recipient of flowers ordered by a friend, and who denies knowledge of their origin. The FTC ruling protects him from having to pay for unordered merchandise, but if electronic data processing can bring together several instances of this individual's receiving "unordered" merchandise, prosecution for fraud becomes much easier.

Another help to successful prosecution is showing that, although an individual transaction is less than the amount prosecutors will pursue, the total of several frauds exceeds the limit. Large numbers get their attention, in other words.

Police Coordination

Small police agencies have one significant advantage over large ones. Criminal investigation is usually better-coordinated because the entire criminal investigation division is often only one detective. When a single investigator "catches" all of the cases, he can easily spot patterns and make correlations.

Large agencies, with large and specialized subsections within their criminal investigation divisions, often suffer from lack of coordination. The narcotics investigators will know the names and working areas of most of the drug dealers in town, but won't pay much attention to addicts

who earn the money for a fix by passing bad plastic. If they apprehend an addict they'll be more concerned with obtaining the name of his dealer than tracking down the source of any fraudulent credit cards he may have in his possession. Narcotics investigators often concern themselves with organized crime connections with the drug traffic, but may be totally oblivious to a possible link with organized crime when they pick up a suspect with a pocket full of credit cards, each in a different name.

The investigator who catches credit card cases, without looking at the possible ramifications, also misses the opportunity for a larger investigation, and more "quality" arrests. Working pawn shops, for example, may bring leads not only to burglars disposing of stolen goods, but may also reveal credit card fraud artists disposing of material. Flea markets can also be outlets. This is why it's worth giving exhibitors at flea markets a once-over.

Working Informers

Every criminal investigator develops a corps of informers. Informers do so for various reasons. Some say for pay. Others try to cut "deals" after being arrested. Some are so treacherous that they'll "roll over" on their friends and partners in crime to obtain special consideration. Yet others do it for revenge.

Informers vary in their reliability and the quality of their information. Officers vary in the use they make of criminal information. An informer can simply provide leads, pointing an investigation in a certain direction. He can provide information on the criminal milieu, or provide information to support an affidavit for a search warrant. The police officer can also turn the informer into an agent, and use him to manipulate a criminal gang into a vulnerable position. This comes about when the agent helps plan a fraud scheme, and informs the police of its progress.

The officer working an informer must understand from the start that it can never be an equal relationship, and that it will always be manipulative. Because informers are criminals first, they try to exploit the relationship in their favor. The alert investigator must always keep the upper hand, playing the informer ruthlessly and without pity.

The investigator who begins to pity his informer, and who wants to do him favors, is beginning to lose control of the situation. Informers are con men, and rely upon exploiting human relationships for their benefit. This is why many police agencies have strict policies regarding informers and how police officers are to treat them.

The procedure for working informers varies with the purpose and with departmental policy. In many cases, it's very informal, with the officer paying the snitch out of his pocket, or overlooking small offenses. In other cases, the agency provides "walking around money" for paying informers, and lays out a specific procedure to follow.

The normal bureaucratic procedure begins, if the subject is an arrestee, with advising him of his rights, following Miranda. To keep it in order, the suspect/informer signs his waiver of rights in front of two witnesses, who sign and date the form.

There is also a personal information form to fill out, to record data which investigators can use to check out the informer and his record. In addition to basic information such as address, employer, age and physical description, the officer should also get the names and addresses of relatives and friends.

When working an informer, it's efficient to obtain as much information as possible from him. This serves two purposes:

1. It makes most effective use of each informer.
2. It also provides a wider base of information for cross-checking, to test a snitch's truthfulness.

Casual questioning may do for a start, while gaining the informer's confidence. The investigating officer should also use an interrogation worksheet to guide him and to record the information. He should ask about other criminal activity, such as auto theft, drug dealing, gambling, prostitution, in addition to credit card frauds.

The agency may also require a formal agreement signed by the informer, covering the conditions of work, and specifically what he's forbidden to do while working as an informer. This is mainly to cover the officers involved in case anything goes wrong, as informers are notoriously unreliable and venal.

There may also be a receipt for money paid to the informer. This is simply for accountability, as some agencies require that all funds be vouchered.

The interrogation worksheet is comprehensive, because it's necessary to work an informer for all possible information. Some informers will spill information, because the officer catches them during a vulnerable moment. They also may have a change of heart, and flee once they're free from custody. This is why it's vital to get everything possible as soon as possible.

Beyond the paperwork is the relationship between the officer and the informer. The officer must be solid and reliable, although the informer appears to be a "flake." This is because the basis of the relationship must be that the officer delivers what he promises. This serves the purpose of the carrot and the stick. If the officer promises a reward for cooperation, the informer must be confident of receiving it if he does his part. If the officer promises reprisals for non-performance or breach of faith, the informer should believe it.

The reward system should be clear at the outset, and the snitch should understand that all reward payments are contingent on the information's being good. The simplest reward is money, because it's legal and under the officer's

control. Offering a "deal" may be tempting, but impossible to fulfill, if formal charges are on file, because the deal requires approval of both prosecutor and court.

The most risky method of payment is in drugs, which is the practice in certain large agencies. Paying in drugs is tempting, because it provides a choke-hold on an addict, and the officer has total control. However, it's illegal, and can wreck a career if it comes to light. Otherwise, diverting drug supplies from other investigations provides the material for payment, and the modest quantities needed are easy to fudge in the inventory. This gives the officer more control, as he does not have to have receipts or vouchers as he does for money.

The investigating officer should be thorough when interviewing his informers. This is both to elicit the most information possible and to pin down the details for cross-checking. He should take down the main points in his notebook, in front of the informer, to let him see that's he's making a record of his statements. The officer should also try to overlap his informers, so that he may cross-check all information among at least two snitches. He should require explanation of all discrepancies.

Testing informers by means of various "truth machines," such as those which record heartbeat, respiration, or even voice pitch, is almost useless. Mounting evidence shows that a minority of people can "beat" these machines, and that many of these people do so precisely because they have criminal personalities. We find more of them in criminal pursuits.

It's important to verify independently all information received. Informers tend to tell their controlling officers what they want or need to hear. Sometimes it's from pure venality, but often it's because the snitch is eager to please. This can cause the snitch to shade the facts, selectively reporting only what he feels his control officer wants to hear.

Another danger is that the informer may change sides again. If his associates suspect his role, they may put pressure on him to feed false information to the investigating officer. This sort of pressure can be very effective, because it's usually backed up by a credible threat of death for failure to cooperate. The snitch may pass false leads to his control, and even plant a listening device if he gets the chance. This is why investigating officers should never trust their snitches completely, never bring them into the office or other sensitive areas, and never tell them anything they would not want their suspects to hear. The basic rule is "get, don't give."[1]

The investigating officer should be watchful regarding his snitch's security. While in the end, snitches are expendable, losing an informer can compromise an investigation, and if the snitch winds up being killed spectacularly, it can deter others who might have considered informing.

This is why meets between officers and informers should be discreet, with both the officer and his snitch watching for surveillance on the way to and from meets. Meets should never be at any police facility. To enhance security, it's better not to have a physical meet, but to use the telephone. This offers better chances of avoiding "burning" the snitch.

The basic technique is to give the informer a telephone number which will always be answered by a telephone answering machine, even though an officer may be next to it when it rings. This prevents callers from hearing anything that may disclose its location, such as background conversation. The recorded message should give the last four digits of the number reached, and say nothing about the location of the number or the office, to avoid giving anything away. A typical uninformative message might be: "6844. Please leave your message when you hear the tone. You'll have one minute." The snitch memorizes the number or carries it on a piece of paper,

with no other notation. This is less compromising if he's searched.

The informer should always act as if his home and work telephones are insecure, and should always call from a public phone. This minimizes the risk of a wiretap. When the snitch calls, he gives a number where the investigating officer can reach him with a call-back. This should also be a public telephone.

If the informer develops into a witness, the relationship becomes more complex because the investigating officer must coordinate it with the prosecutor, and make arrangements for immunity, if that is an issue. There may also be a need to provide physical protection for the informer/witness, as some large rings may undertake to have him killed to forestall his testifying. Overall, it's awkward to use a criminal informer as a witness, because a defense attorney can easily cast doubt upon his testimony by questioning him as to his motives. If the witness is testifying in return for immunity, it may appear that he's simply trying to save his own skin. If for pay, he appears mercenary.

Some informers develop into career snitches, passed from agency to agency as their usefulness fades in each locale. This is why it's worth asking the informer at the outset if he'd be willing to work for another officer or agency, and on what terms.

Despite recent technical advances in police science, the human element can still be useful. Informers, when used for obtaining information unavailable elsewhere, and for developing leads, are among the most helpful tools an investigating officer can have.

Luck

Luck certainly plays a part in some investigations. Investigators can help their luck by maximizing the chances of a stray event's bringing useful results. It's luck if a credit card passer is stopped for a traffic offense, but the officer may not recognize the offender as one who is wanted. However, if the department's equipped with mobile data terminals, and criminal investigators enter all information into the central computer quickly, the picture changes.

Working Up The Chain

Once the entry into a case comes, it's worth a maximum effort to exploit the opportunity. A fraudulent credit card passer arrested in the act can provide information about his sources of supply. A drug addict can describe how he obtains the money to support his habit. Each of these is a link in a chain, and the investigator or his team must work their way up the chain to other links.

Some drug addicts offer an opportunity for quick exploitation, because of the hold their habit has upon them. The addict on morphine, heroin, demerol, or other opiate is vulnerable to withdrawal. Arrest means separation from his source, and the onset of withdrawal symptoms is often within a few hours after arrest. The officer who offers to take the addict to the hospital emergency room in exchange for names can make a good bargain. However, the officer who provides drugs directly is risking his career.

Search Warrants and Raids

The raid is a means to execute a search and obtain evidence. In many cases, a search warrant is necessary. Exceptions are when the situation demands immediate action and there's no time to obtain a warrant, such as when the offenders are preparing to flee and to take the

evidence with them. Hot pursuit, self-protection, and permission to search from the owner of the premises are other instances justifying warrantless searches.[2]

A search warrant affidavit can be a ball of wax. There's a requirement of "probable cause" that may be hard to meet. In some investigations, probable cause is often very easy or very hard to find. If the stolen property is on display at a flea market, second-hand store, or other place open to the public, an investigating officer can use his own direct knowledge in the affidavit. If the merchandise is not on view, he may have to rely upon an informer.

Relying on informers to justify a search is bad practice. Some judges don't place much faith in informers, and may deny a warrant based on such a source alone. This makes it necessary to engage in "judge-shopping," to find a cooperative judge. Such a judge may not be available when needed.

Occasionally, an investigation won't be able to wait for a search warrant. The investigator must scramble for probable cause to search a building or vehicle. In some jurisdictions, one way to obtain probable cause is the practice known as "dropping your own dime." This involves telephoning the police emergency number and reporting a "man with a gun" in the vehicle or building. Once the call comes on the air, the investigator reports himself as the nearest unit, and responds.[3]

Occasionally, the raid will fall into the "high-risk" category. This is especially true if narcotics are involved, and if the suspect premises also house a drug processing laboratory or similar facility, the suspects will probably have heavy weapons. This situation calls for support from a S.W.A.T. team, who may form part of the raiding party or remain in the background unless needed. If it's clear that armed resistance is likely, S.W.A.T. officers may form the first wave, as they are experienced in forced entries.

Imagination

Although it may seem a mundane task, credit card fraud investigation is challenging and sometimes exciting. The main point seems to be having the judgment to separate the worthwhile investigations from the dead ends, and the open mindedness to follow up forcefully. This often requires imagination, and the clever investigator will find that clever work brings results.

Sources

1. *Notable Crime Investigations,* William Bryan Anderson, Springfield, IL, Charles C. Thomas, Publisher, 1987, pp. 67-68.
2. *Raids,* James Martin Davis, J. D., Springfield, IL, Charles C. Thomas, Publisher, 1982, p. 102.
3. *Buddy Boys,* Mike McAlary, NY, Charter Books, 1988, p. 75.

Part III

Tools

This section will cover specific items of equipment and their use in the investigation of credit card fraud.

10

Tools For The Job

Copy Camera

Sirchie Fingerprint Laboratories sells several types of fingerprint cameras which are designed to produce 1:1 (same size) photographs of fingerprints and other evidence. They also double as copy cameras for small documents. The Model EVC-1000 accepts a Polaroid 3¼" x 4¼" film pack, and produces black & white or color copies. The Models 2000 and 3000 accept 4" x 5" Polaroid film packs, which are actually larger than necessary to copy drivers licenses and other card I.D. documents.

Copy cameras are useful for copying evidence. As credit card fraud usually involves small items, the copy camera fills a gap left by the photocopy machine, which typically copies only in one color.

All models carry their own electronic flash, powered by rechargeable batteries. Exposure control is both by adjusting the aperture and the flash brightness. Prices are between $800 and $1,000, depending on the model. Cameras are available from:

Sirchie Fingerprint Laboratories, Inc.
P.O. Box 30576
Raleigh, NC 27662
Phone: (800) 356-7311

Reference Manuals

The Ball-point Rip-off: A Forgery Investigator's Handbook, Detective K. Olson, Santa Cruz, CA, Davis Publishing Company, 1975.

Credit Card Fraud Control Manual, American Bankers Association.

How To Protect Your Business, Neil W. Sandler, Elmsford, NY, The Benjamin Company, 1985.

11

Information Management

Although it's fashionable to call it "intelligence," it's simpler to use a word we all understand: "information." Credit card fraud prevention and investigation requires comprehensive information management for several reasons:

- The number of crimes is more than the numbers of other categories, such as robbery or murder. This means that individual crimes get less individual attention from investigators. In fact, some agencies have cut-off limits below which they will not pursue a case because they have their hands full with larger-volume crimes. We also see this in the limits imposed by law, with Postal Inspectors not getting involved unless the annual total exceeds $1,000.
- Information is available from more sources than in certain other types of crimes, and it's necessary to collect, categorize, and index this information to make it useful. Private sources are very helpful in this regard.
- There are several useful ways of categorizing information to detect patterns and obtain leads. This is very important, because credit card fraud, like many property crimes, very rarely shows a personal link between perpetrator and victim.

Unfortunately, many agencies are caught between an increasing number of reported crimes and shrinking budgets, and for this reason, can't cope. Officers then take only minimal information, such as time, date, description of the perpetrator, and the credit card slip. This offers slim chances of clearing the case.

Agencies which can gather more information will find it rewarding. After a certain point, crime information helps turn the tide against credit card fraud, as we'll see.

Types of Information Available

Crime Reports

These are the raw material of many information files, and making full use of what they contain is a vital first step. Many credit card frauds are not reported to police until days have passed, because the paperwork hasn't cleared, and the merchant is unaware that anything is amiss until he gets a chargeback. The trail is then cold, and sales clerks may not remember anything about the transaction. This is what makes each available report important.

Another type of crime report worth listing is anything touching upon credit card loss or theft. A burglary in which the victim reports his credit cards stolen is worth listing. Likewise, ATM armed robberies, normally handled by the robbery detail or major case squad, are relevant to credit card fraud investigations. This requires close cooperation, not rivalry, between various squads and divisions in a police department.

Physical Evidence

This includes the charge slip, if available. Unfortunately, perpetrators' fingerprints are rarely recoverable from charge slips. In telemarketing fraud, there's nothing tangible from the person placing the telephone order, but there may be a delivery receipt.

Criminal Information

This can come from calls to "Crime Stop," professional "snitches," from suspects seeking a deal, or others informing out of jealousy. One example comes from the school liaison officer, in jurisdictions which have them. Juveniles who purloin parents' credit cards often openly display stolen goods to each other, trade items, and sometimes will snitch on each other out of jealousy.

Organizing the Information

This is the vital first step, for both police and private agencies. Private agencies can use this information to prevent and to recover losses. Police agencies can use the information in pursuit of credit card defrauders, and as collateral information in other investigations. As we've seen, credit card fraud doesn't occur in a vacuum, and officers may be able to link it with other crimes.

Much electronic data processing is donkey-work, and it's profitable to use this as "filler" work if there are any slow periods. It's also a way of training officer cadets and probationary patrolmen. Much police work is shuffling papers, and they can use this for an early start in their careers.

There are several useful approaches to categorizing the information, by people involved in the crimes, the crimes themselves, and overlaps with other crimes. All ways are adaptable to paper and electronic methods.

People Information

This includes information about two types of people: (1) those with prior convictions for credit card fraud, receiv-

ing stolen goods, and document forgery, and (2) those whose names turn up in investigations but who haven't been convicted or even suspected. This category includes victims, their families, witnesses, employees, etc. It's a catch-all category because at times certain patterns can show up by including people without criminal records.

A hypothetical example might be a series of credit card frauds in which genuine cards made out to nonexistent persons had been the instruments of fraud. This suggests an "inside" aspect, with an employee furnishing blank credit cards to the suspects.

Information to include in each entry is different from the usual type of personal information file. A suspect may not have a fixed address or employment. Many are nomadic, and some have a fixed address for several years at a time (prison). Others typically use accommodation addresses, or mail drops. This is why it's very helpful to concentrate on names and addresses of family members and friends and associates. Locating the person often requires working through friends and relatives. To this end, it's also helpful to include cross-references in an appendix to each file.

Addresses can be very important in investigating various forms of telemarketing fraud. This information can both help to pin-point the identity of the perpetrator, and to establish the pattern of fraud. A computer "run" on every address involved in a fraud can show that several deliveries went to the same address, even though the name on the credit card was different in each case. A second-order run may show that a group of addresses are all linked to the same person, belonging to friends or relatives, thereby establishing a pattern.

The personal file format, whether for paper filing or electronic database, should include at least these categories:

Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars
Status (convicted, suspected, victim, witness, etc.)
Occupation
Last known employer, including address, telephone, and superior

Closest relative:
Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars
Status (convicted, suspected, victim, witness, relative, etc.)
Occupation
Last known employer, including address, telephone, and superior

Another relative:
Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars
Status (convicted, suspected, victim, witness, relative, etc.)
Occupation
Last known employer, including address, telephone, and superior

Another relative:
Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars
Status (convicted, suspected, victim, witness, relative, etc.)

Occupation
Last known employer, including address, telephone, and superior

Closest friend:
Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars
Status (convicted, suspected, victim, witness, etc.)
Occupation
Last known employer, including address, telephone, and superior

Another friend:
Name
Last known address
Telephone
Date of Birth
Social Security number
Sex
Height
Weight
Hair color
Eye color
Distinguishing marks or scars

Status (convicted, suspected, victim, witness, etc.)
Occupation
Last known employer, including address, telephone, and superior

It won't be possible to obtain all items of information about every person contacted or interviewed. However, even partial information is helpful and often is enough to provide a link.

Crime Information

This is what's normally called the "M.O." or modus operandi, Latin for "method of operation."[1] The value of the M.O. is that credit card artists tend to operate in a pattern; they get in a rut or find one way of working that appears to work best for them. Some specialize in department stores. Others work telemarketing services. Yet others travel a lot, paying for air fares and accommodations with plastic. Some use credit cards as an adjunct to motor vehicle theft. Listing the M.O. can suggest a list of suspects.[2]

The minimal information should include:

- Type of fraud — retailer, travel industry, car rentals, etc.
- Location — urban, rural, suburban.
- Time of day.
- Nature of goods or services.
- Description of suspect, if seen.
- Type of vehicle used, if known.
- Does anything about the case suggest inside information?
- Collateral crimes — was there an assault or other crime committed to facilitate the fraud? Do the credit cards used connect with another type of crime, such as burglary?

The Mail Drop and Address File

Criminals often use addresses other than their own to list on official documents, and to receive stolen goods, if they're using a telemarketing scam. In many cases, it has to be an address where they can receive mail and shipments.

One type of service that serves the purpose very well is the commercial mail drop. These are private postal service boxes which operators rent by the month or quarter, and which fraudulent credit card users list as mailing or shipping addresses. Although the U.S. Postal Service requires mail drop operators to list I.D. presented by the renter, in practice this is meaningless. Mail drop operators simply request I.D., and truly don't care if the I.D. is genuine or not. They cover themselves by filling in the blanks in the postal service's printed form. This allows fake card passers to use forgeries of indifferent quality.

There is a commercially printed list of mail drops, *Directory of U.S. Mail Drops,* which is revised every two years. This is available from:

Loompanics Unlimited
PO Box 1197
Port Townsend, WA 98368

This list is very incomplete, although it contains an appendix for foreign countries, and serves only as a starting point for the mail drop file. A more current listing is available in the telephone directory's yellow pages, under "Mail Receiving Services." This is brought up to date each year, and lists all mail drops in the local area.

At times, fraud artists may use addresses of friends or relatives. They may choose to do so because it's more convenient, or simply cheaper. It's worth listing every address associated with this sort of fraud, or with bad checks, to cross-check if the address turns up again during a request for authorization or an investigation. Any

sort of association is worth listing, because it can provide a link with another fraud, perpetrated in the past. An example is the con artist who uses a genuine card, in his own name, to have merchandise delivered to a confederate who then claims he never received it. Not receiving a delivery may be credible once, but if a pattern develops, it's obviously fraud.

A retailer may request a check on every address given by customers paying by credit card. It may take only a few seconds, depending on the address and the size of the database, to run an address check, but during busy days it may be possible only to spot-check. If the database is in a manual card file, it takes longer, and the index will be smaller for a given amount of space. With a computer, as we'll see, a significant improvement in speed is possible.

A "hit" on such an address is not proof of fraud, but merely a suggestion for caution. There are legitimate reasons for using a mail receiving service, one being a precaution against mail and package theft for people who are away from home during the day. Likewise an address listed under suspicious circumstances may have a new occupant, unrelated to the previous one. A history of "failed deliveries," for example, can point to fraud if the same party still lives at that address. If the receiver has been clever enough to use different names, it won't be as clear.

Proper follow-up to a hit is essential. If the address provided by the customer turns out to be a mail drop, the clerk or manager should ask the customer point-blank; "Is this your home address?" A deception at this point merits further investigation.

Making Information Work For You

Correlating information and having it available for instant retrieval is the big leap, but to get the most out of this it's necessary to have a computer. Large agencies

have had computerized criminal files for years, and the National Crime Information Center, (NCIC), has been in operation for almost two decades. Today, small personal computers, "PCs," are in almost every police station in the country. Making the best use of these requires a "database" system. Fortunately, these are easily available and affordable.

A database is an electronic filing system. It allows entering a great number of names, addresses, and information in a number of categories, and recovering them quickly and in different combinations. This makes a search for information very quick, if the information is on file in the system.

There are many databases available, and some are very expensive, as high as $700, while others are in the public domain or are "shareware." "Shareware" is a system in which the disk with the program is available for free distribution, or at nominal cost, and users are on the "honor system," paying if they find it useful.[3] Others are available on the commercial market at fairly low cost, and it should not be necessary to pay more than about $150 maximum.

Adapting a database to this use isn't very difficult. The first rule is that you can't retrieve information you don't punch in. Theoretically, it's possible to compile a list of one-armed bad card passers convicted in Alaska who graduated from dental college and flew to China on vacation, but only if all of that information is on file. It's necessary to decide what information is worth saving, and what can be left to paper files.

"Keyboarding" will be a massive task at first. This is the laborious and unrewarding stage of converting to computerized operation, when there's too little information in the files to give much useful output.

How many entries can a database hold? Strangely, the cost of the database program doesn't have much to do

with capacity. This depends on the size of the entries and the capacity of the disk. As a very rough guide, a file listing only name, address, and telephone number takes about 100 to 200 "bytes." Double-sided, double-density 5¼" disks have a capacity of 360,000 bytes, which allows about 3,000 such entries. A file using entries like the one illustrated above will hold fewer than 1,000 per disk.

An improvement comes with double-density 3½" disks, which hold 720,000 bytes. These require a DOS version 3.3 or higher. The "HD," or High Density, loading, requiring special disks, takes 1,400,000 bytes. These cost at least twice as much as regular 3½" disks.

There are ways of shortening entries. One is to assign code numbers. The field ARREST CATEGORY can take up many letters, as in the entry "American Express Card fraud," but if these categories can be reduced to two-digit numbers, it will save a lot of space and partly encode the information, providing a slight degree of security. A short list may be as follows:

01-Credit Card Fraud, Retail

02- Credit Card Fraud, (Vehicular Theft)

03- Credit Card Fraud, (Bust-out)

04- Armed Robbery, ATM

05- Possession of Falsified Driver's License

06- Forgery of Official Documents

07- etc.

With such a simple system, it's possible to use the two-digit code to replace up to 99 different entries of over two dozen letters each. A quick way to compile such a list and to commit it to memory is to use the last two digits of penal code entries where possible. This will make use of numbers already memorized for many entries.

It's possible to encode everything, but not very practical. The above-listed system will also work for CONVICTION CATEGORY, but other fields don't easily lend themselves to this type of coding. It's also possible to reduce the modus operandi entries into two-digit codes, for quick reference. Some categories that are workable for two-digit entries are type of credit card fraud, (airline, restaurant, retail merchant, etc.), sex of perpetrator, and type of supporting documentation (drivers license, check guarantee card, employee I.D. card) etc.

Eventually the files will become too bulky for a single disk. This is the point at which it's necessary to break off part of the file for transfer onto another disk. The first disk will still retain entries starting with letters A-L, and the second will have those starting with letters from the rest of the alphabet. It helps to plan for this right at the start, because if any radical changes in the file system become necessary, it may be necessary to re-type all or most of the entries.

Sorting the files by type of crime and M.O. is the best way, rather than alphabetically or geographically. This enables the best cross-referencing between individual entries. The weaknesses of other methods are quickly apparent.

If the files are alphabetical, by last name, a gap opens up once it's necessary to divide them into two or more disks. A person with a name beginning with "B," for example, "Brown," may have an alias of "Smith," but this will be on another disk if the first only goes to "L." If there's a search by address, the search will miss one of the aliases, unless the searcher does both disks.

The exception is with addresses associated with credit card crime. This is usually a small and manageable number of addresses, and will fit easily on a disk.

Two more points about electronic storage:

- Back everything up. This means making duplicates of your disks and storing them in a safe place away from

the office. This reduces the danger of destruction through fire and other accidents.

- A "hard disk" contains much more information than a "floppy." These are available in a number of sizes, from ten megabytes to forty and more. This makes handling the information much quicker. It's just as vital to back up a hard disk as a floppy. If the disk "crashes" or suffers other damage, you lose even more information.

Searching through the files electronically is a very precise operation. There are several modes of search available. One is a simple scan, which will find a certain name or set of numbers. For example, if you need to find all of the Smiths in an area, you can simply type in "Smith." This will scan all last names for five letters. It will also pick up any "Smithfields," and "Smithsons." If there are many similar names, it's possible to speed up the process by typing in only the first three, "Smi."

When searching for an address, typing in only the first few digits and the city will probably be the fastest way of recovering a match. Granted, there are similar numbers on parallel streets, but when searching a limited category, such as mail drops, it's very unlikely that many mail drops will occupy the same address numbers on these streets.

Likewise, in searching for all crimes following a certain M.O. in a geographical area, it's possible to go by code number. Typing the number will bring up all of the entries in that area.

Another type of search is the "full-field" search. This will find a few letters or numbers wherever they may appear. If, for example, you have to seek out an address from a number recalled by a witness, you may have only the house number, or a part of that. If it's "333," you type that in, and the program will bring up all entries with an address that begins with "333."

You may also have only part of a name. This means that you must make a "generic" search. Typing in the letters involved will bring up any name with those letters occurring in that order, whatever position they occupy.

Finally, there's the "soundex" search. This finds all entries that sound like the name you typed in. If you type "Smith," you also get back names such as Schmidt, Smyth, Schmitt, and Smit.

Finding a name, address, or other cross-reference is helpful, but a full follow-up must direct the seeker to the right paperwork file. Simple filing programs for small computers are rudimentary, and have no capacity for photographs as do the computer filing systems that cost big bucks. These, and much additional information, has to spill over into paper files. Every entry must have a reference number or other information which will connect immediately to whatever paper record exists on the person.

Evaluating

Stockpiling information and drawing relationships are the initial steps. Evaluating the information is the next. This always requires a human operator, because there are subtle judgments to form which are beyond the ability of any machine.

An arrest record is, of course, an alert sign, regardless of the disposition of the case. So is a "suspicion" record, however tenuous it may be. This might have come about because the individual was an employee of several different firms at the times they suffered extensive credit card victimizations. If there's an entry for having been on a "suspect list" for a bad check or credit card, this merits a closer look if the same person appears on the suspect list for another crime. The M.O. file will probably be very useful, but so will a simple list of suspects not confined at the moment.

A problem with maintaining a suspect list is that civil libertarians will consider it a "police state" measure and an infringement of individual rights, if they find out. They can also point out that being employed by a firm fallen victim to a crime is not a crime in itself, and that police should not keep detailed records. This a strong reason for keeping the database under a tight lid of secrecy, and allowing access to the fewest persons possible.

This is not too difficult for a police agency, and very easy for a private agency or company. The Bill of Rights exists, after all, to protect citizens from the government, not other citizens.

Security

Only one person, if possible, should be able to retrieve data from the file. There are encryption programs to disallow access to anyone who doesn't have the "password."[4]

A further security step is for the investigator to take the disks home with him each night. This can become cumbersome, and is not a substitute for encryption, because it's easy to forget the disks at one time or other. Because many people have home computers, it may be possible to use the computer at home, instead of bringing the data to the office. The work is such that it can be done at home, returning the papers to the department's files the next day. This requires the permission of higher authority, but this should not be hard to get after communicating the purpose.

Inter-Agency Cooperation

Credit card rings are far-reaching, often crossing state lines, and many are beyond the ability of any single

agency to handle effectively. Individual card passers can be very fast-moving, because they know that mobility keeps them one or more steps ahead of the law. In many instances, there is information available to aid an investigation, but it's resting in a file several jurisdictions away. At times, an area-wide task force may be the best solution, but not likely to arise.

There are several purposes to the task force, however. On one level, advising each member agency of current investigations will alert them to areas where they might provide help. Another area for mutual help is dividing the workload. With limited man-hours available, avoiding duplication will make the most effective use of the resources.

Another way of sharing information is to pass a "shopping list" between agencies. This is a listing and brief description of current cases, with a note attached requesting that any agency with information pertaining to these cases transmit it to the investigating agency.

A database becomes more effective with increasing size. Small agencies can never, by themselves, build up large enough databases to be truly useful. Credit card fraud can take in a large geographical area, overlapping jurisdictional boundaries. A car thief lives in one jurisdiction, rents cars with a fake card in several others, and drives them to yet another. This is why it's vital to establish a central information facility.

The central database may be in the custody of the largest agency in the region. While this does have a "big daddy" aspect, experience has shown that it's a workable plan. State criminal information computers and motor vehicle bureaus work well, and are accessible to the smallest agencies.

An alternate plan is a cooperative effort, with a small multi-agency office to house the information. In either case, the practical way to do it is with a computer.

Electronic data management works for quick filing and retrieval. Once investigators focus on a specific person or case, they can obtain the paperwork by conventional means. Electronic data management is a time-saver.

Use of a "modem" in conjuction with telephone lines provide a practical way for agencies to gain access to the central computer. A modem is an electronic device for transmitting and receiving information between computers. Modems are inexpensive these days, basic models costing less than $100, and upgrade models somewhat more.

Properly handling information can make a huge difference in the effectiveness of law enforcement. The mechanism can be a central clearing house, as we find with auto thefts, or it can be decentralized, as with confidential intelligence files. Either way, its effectiveness depends upon the diligence of the investigators who operate the system.

Sources

1. *Fundamentals of Criminal Investigation,* Charles E. O'Hara and Gregory L. O'Hara, Springfield, IL, Charles C. Thomas, Publisher, 1981, p. 658.
2. *Criminal Investigation,* Paul B. Weston and Kenneth M. Wells, Englewood Cliffs, NJ, Prentice-Hall, 1974, p. 110.
3. A source for such programs is:
   PC Software Interest group (PC-SIG)
   1030 E. Duane Ave, Suite D
   Sunnyvale, CA 94086

   Try the low-cost public domain and "shareware" databases first. These cost about six dollars per disk. One is File Express, listed in the PC-SIG catalog as disks #287 and 288. Another is disk #119, the ABC Database. Yet another is PC-FILE, but this one has a catch. The disk is available at nominal cost, but the instructions on the disk are purposely incomplete. This prevents you from getting much use from it unless you send the manufacturer the fee he asks.
4. One encryption program is Computer Security Encryption Package Version 1.53, available as disk #112 from PC-SIG. This blocks access and has a program to detect tampering.

Glossary

Account A sum of money, deposited with a bank, against which the account holder can make withdrawals. With a checking account, the client writes checks as payment orders, allowing third-party withdrawals for the amount of the check.

Alias A false name assumed by a person.

ATM See Automatic Teller Machine.

Authentication Any way of verifying that the person presenting a card, check, or other document is the authorized bearer or customer. This can be with a password, number, signature, or other means.

Authorization In this context, permission from the issuer to the merchant to accept a particular charge transaction. The issuer usually requires authorization for transactions above a particular amount, known as the "floor limit."

Automatic Teller Machine An electro-mechanical device that dispenses money and accepts deposits by a customer who inserts a bank card into a slot and punches in a PIN for authentication.

Bearer A person presenting a check, credit card, or other legal instrument for payment.

Bustout An organized fraud in which the perpetrator uses an existing company's line of credit to purchase inventory and services, and then disappears. This is also called: "take the money and run."

Card-holder The person whose name appears on a credit card. This is usually the bearer.

Chargeback A debit against a merchant's account by a credit card issuer. This may come about because of an invalid card or other problem that the merchant could have prevented.

Check A printed form, issued by a bank, which is a payment order payable on demand when properly filled out and signed by the account holder.

Check cashing card A card, issued by a bank, which guarantees a check up to a fixed amount. The bank promises to pay the subscriber the face value of the check, as a protection against forgery or misuse. This is also a convenience for retail clerks, who only have to note the guarantee card's serial number on the check.

Check digit A number, usually at the end of a card identification number, that serves as a control over possible forgery. The check digit is derived from a very simple formula, and allows anyone who knows the formula to work it out to ensure that the number is genuine.

Check guarantee card See "Check cashing card."

Check protector See "Check writer."

Check writer A desk-top machine which prints and embosses the amount set on its dials. Used to prevent alteration of the face amount on a check.

Counterfeit A falsified or forged document, including currency, checks, bonds, and coins.

Credit slip Printed forms used to make credit card payments.

Float A term denoting uncollected funds in transit.

Floor limit The amount of a purchase which requires prior authorization by the credit card issuer.

Fraud Obtaining money or goods by trickery.

Guarantee card A type of identification card, not negotiable in itself, which serves to guarantee a merchant from loss if he accepts a check written to the account on the card. Some bank credit cards also serve as guarantee cards.

Hold An administrative order placed upon an account, preventing payment of any checks until the amount represented by a deposited check is collected. In other words, the bank does not pay any check until the deposit "clears."

Holograph An image, laser-printed on a metal foil surface, which appears to change color or shape with the viewing angle. Also "hologram."

I.D. Any identification document, such as a drivers license, bank card, birth certificate, etc.

Issuer The bank or company which issues a credit card.

Keybook The printed guide to American Bankers Association routing numbers.

Kiting A check fraud scheme in which the con artist writes checks alternately against two accounts, covering each check by another check deposited into the account. This is also possible with credit card accounts.

Mail drop A mailing address which is not the person's residence. Mail drops are often means to facilitate fraud, providing a con artist with an appearance of legitimacy, and breaking the trail of an investigation.

Merchant Any retailer who accepts credit cards as payment or as check guarantee cards.

Personal Identification Number Any combination of letters or numbers that identifies the card-holder. The customer should retain the "PIN" in memory only, to prevent its discovery by unauthorized persons.

Questioned document A suspected document. This may be a check, credit slip, driver's license, or other document under suspicion.

Questioned document examiner A specialized criminalist who examines suspected documents in a laboratory for evidence of authenticity or forgery.

Restitution Reparation for loss.

Routing system A system, using alphanumeric symbols, used to direct transactions between banks.

Statute of limitations Time limit on filing criminal charges for a specific act.

Supporting documents Additional identification documents (I.D.) presented when paying by credit card or check.

Index

Addicts, 86, 87, 90, 93
Air travel cards, 15
Airline tickets, 48, 53
Alterations, 24, 29, 33, 77, 78, 122
American Bankers Association, 1, 7, 27, 123
American Express, 3, 11, 12, 17, 49, 53, 112
ATM, (Automatic Teller Machine) 8, 13, 14, 15, 26, 37, 43, 44, 46, 47, 112, 121
ATM cards, 13, 15, 44, 46, 47
ATM frauds, 46, 47
ATM robbery, 43, 44, 102
Authentication, 121
Auto theft, 54

Background checks, 49, 73, 75
Bank cards, 14,16, 37, 56
BIN number, 24, 79
Blank slips, 55
Bust-out, 56, 80, 82, 112, 122

Carte Blanche, 12
Cash advances, 56
Charge slips, 18, 19, 20, 22, 24, 42, 51, 55, 77, 78, 80, 82, 102
Charge slip carbon, 50, 79
Charge-backs, 2, 52, 102, 122
Check digit, 23, 24
Check guarantee cards, 17, 29, 30
Checkbooks, 46
Chemical eradicators, 23
Company credit cards, 55, 56
Computer database, 83, 86
Consumer victimization, 61
Conversion frauds, 52
Copy stand, 32, 34
Corrupt employee, 62
Credit card blanks, 36, 37, 104

Credit card passers, 2, 19, 35, 41, 42, 45, 46, 48, 49, 52, 53, 63, 68, 72, 76, 77, 79, 82, 93, 109, 111, 117
Credit card slips, 49
Credit doctors, 57
Crime report, 102

Database, 77, 82, 104, 110, 111, 116, 117, 118, 119
Debit card, 15
Diner's Club, 3, 11, 12
Direct merchandise frauds, 47
Dishonest merchants, 55
Divorce-related buying spree, 47, 48
Drivers license, 25, 33, 34, 78, 99, 112, 123, 124

Electronic data processing, 103
Embossed numbers, 24

FBI, 67
Fictitious charges, 63
Fine-line printing, 24, 25
Fingerprint, 34, 99, 102
Floor limit, 19, 48, 78, 82
Forgery, 22, 23, 28, 29, 30, 35, 38, 41, 48, 58, 77, 100, 104, 109, 112, 122, 124
Fraud against a customer, 7
Fraud by a customer, 7
Fraudulent applications, 49, 50

Gift certificates, 25, 35, 38, 53, 54
Grace period, 45, 54, 58

Holograms, 27, 29, 123
Honesty tests, 73
Hot list, 18, 26, 81

Informers, 87, 88, 89, 90, 91, 92, 94. *Also see "Snitches."*
Inside job, 35, 46
Insiders, 29, 36, 37, 61

Juveniles, 47, 103

Late billing, 61
Learners permit, 34, 78
Lost wallet, 44, 45

Magnetic stripe, 27, 28, 30
Mail drops, 34, 49, 50, 104, 109, 110, 114
Mail theft, 7, 45
Merchant collusion, 54
Metallic ink, 25
Micro printing, 25
Micro-chip, 27, 28
Microprocessors, 27
Mobile criminal, 67
Modus operandi, 108

Non-violent crimes, 21, 67

Oil Company credit cards, 16
Organized crime, 37, 56, 87

Photo I.D., 25
Photocopy machine, 25, 35, 38, 99
Physical evidence, 102
Pick-pockets, 44
PINs, 26, 47
Polaroid copy, 33, 34
Postal Inspectors, 67, 101
Private agencies, 103, 116
Process camera, 31, 38

Retail precautions, 72
Retail store charge card, 16
Retailers, 3, 12, 16, 19, 21, 35, 52, 72, 80, 85, 108, 110, 123

Security measures, 22, 23, 29, 37, 76
Security officers, 22, 36
Shell Company, 82
Signature forgery, 22
Signature strip, 22, 23, 33, 45, 77
Silk-screening, 30, 31, 33
Smart Card, 27
Snitches, 90, 91, 92, 103. Also see *"Informers."*
Stolen credit cards, 18, 22, 23, 26, 49, 54, 71
Stolen drivers license, 33
Stolen goods, 50, 87, 103, 104, 109
Supporting documents, 25, 29, 30, 33, 34, 37, 42, 71, 77, 80, 82

Telemarketing, 24, 50, 51, 54, 67, 78, 102, 104, 108, 109
Telemarketing frauds, 50, 51
Telephone credit card, 54
Telephone florists, 51
Travel and Entertainment Cards, 11, 12

Ultra-violet Ink, 25

Warrant, 87, 93, 94
Watermarks, 25, 38
Witnesses, 3, 88, 92, 104, 105, 106, 107, 108, 114

YOU WILL ALSO WANT TO READ:

☐ **61111 COUNTERFEIT I.D. MADE EASY, *by Jack Luger.*** A step-by-step guide on how forgers make these authentic-looking documents: photo I.D., drivers licenses, birth certificates, credit cards and more. Written by a professional in the printing and graphic arts trades, this book takes you into the basements and workshops of professional forgers to reveal their techniques. ***1990, 5½ x 8½, 137 pp, illustrated, soft cover.*** **$14.95.**

☐ **61098 BIRTH CERTIFICATE FRAUD, A Report *by Richard P. Kusserow, Inspector General.*** This US Government report covers birth certificate fraud. It deals with The Problems, The Issuing Agencies, The Birth Documents, The Issuing Procedures, The User Agencies, and Recommendations for controlling birth certificate fraud. This is the latest information on what the US Goverment knows about fake I.D., and how it is trying to stop it. ***1988, 8½ x 11, 36 pp, illustrated, soft cover.*** **$8.00.**

☐ **49021 FRAUDS, RIP-OFFS AND CON GAMES, *by Victor Santoro.*** Here is another fine book by the master of revenge. Contents include: The Dirty White Collar, Securities Swindles and Theft, Restaurant Scams, Credit Cards: Cons and Catches, Fraud Salad: An Assortment of Con Games, and much more. The woods are full of wolves — don't be a sheep! ***1988, 5½ x 8½, 188 pp, soft cover.*** **$11.95.**

And much more! We offer the very finest in controversial and unusual books — please turn to our catalog announcement on the next page.

CCF

LOOMPANICS UNLIMITED
PO Box 1197
Port Townsend, WA 98368

Please send me the titles I have checked above. I have enclosed $ (including $3.00 for shipping and handling).

Name _____

Address _____

City/State/Zip _____

(Washington residents please include 7.8% sales tax.)

"Yes, there are books about the skills of apocalypse — spying, surveillance, fraud, wiretapping, smuggling, self-defense, lockpicking, gunmanship, eavesdropping, car chasing, civil warfare, surviving jail, and dropping out of sight. Apparently writing books is the way mercenaries bring in spare cash between wars. The books are useful, and it's good the information is freely available (and they definitely inspire interesting dreams), but their advice should be taken with a salt shaker or two and all your wits. A few of these volumes are truly scary. Loompanics is the best of the Libertarian suppliers who carry them. Though full of 'you'll-wish-you'd-read-these-when-it's-too-late' rhetoric, their catalog is genuinely informative."

—THE NEXT WHOLE EARTH CATALOG

THE BEST BOOK CATALOG IN THE WORLD!!!

We offer hard-to-find books on the world's most unusual subjects. Here are a few of the topics covered IN DEPTH in our exciting new catalog:

- *Hiding/concealment of physical objects! A complete section of the best books ever written on hiding things!*
- *Fake ID/Alternate Identities! The most comprehensive selection of books on this little-known subject ever offered for sale! You have to see it to believe it!*
- *Investigative/Undercover methods and techniques! Professional secrets known only to a few, now revealed to you to use! Actual police manuals on shadowing and surveillance!*
- *And much, much more, including Locks and Locksmithing, Self-Defense, Intelligence Increase, Life Extension, Money-Making Opportunities, and more!*

Our book catalog is 8½ x 11, packed with over 500 of the most controversial and unusual books ever printed! You can order every book listed! Periodic supplements to keep you posted on the LATEST titles available!!! Our catalog is free with the order of any book on the previous page — or is $3.00 if ordered by itself.

Our book catalog is truly THE BEST BOOK CATALOG IN THE WORLD! Order yours today — you will be very pleased, we know.

LOOMPANICS UNLIMITED
PO BOX 1197
PORT TOWNSEND, WA 98368
USA

Did you know that someone can drain your bank account using your cash machine card *without your secret code?* Or that clever criminals can get a full month's use from a stolen credit card before arousing any suspicion?

These are some of the startling facts revealed in ***Credit Card Fraud,*** by police writer Burt Rapp. This is a practical manual on defending yourself. It was written for police officers working an investigation and for those stung by credit card fraud: the merchant, the banker, the man on the street.

Why is credit card fraud one of the fastest growing crimes? Because cards are easy to get and easy to steal. Because police don't have the resources to chase these crooks. Because most institutions accept the losses as "the cost of doing business." Only now, the costs are going sky high.

Credit Card Fraud reveals *all* the scams, from forged bank cards to telemarketing rip-offs. It shows the security measures built into credit cards and tells you how to detect frauds. And it explains what businesses and individuals must do to keep from becoming victims.

ISBN 1-55950-055-7